

EXHIBIT A

Patricia L. Peden, Esq. (SBN 206440)
ppeden@bwsllaw.com
BURKE, WILLIAMS & SORESENSEN, LLP
1999 Harrison Street, Suite 1650
Oakland, CA 94612
Phone: (510) 273.8780
Fax: (510) 839.9104

Christopher J. Lee (*pro hac vice*)
clee@leesheikh.com
David J. Sheikh (*pro hac vice*)
dsheikh@leesheikh.com
Brian E. Haan (*pro hac vice*)
bhaan@leesheikh.com
Ashley E. LaValley (*pro hac vice*)
alavalley@leesheikh.com
Dragan Gjorgiev (*pro hac vice*)
dgjorgiev@leesheikh.com
James D. Mitchell (*pro hac vice*)
jtmitchell@leesheikh.com
LEE SHEIKH & HAAN LLC
125 South Clark Street, Suite 1175
Chicago, IL 60603
Phone: (312) 982-0070
Fax: (312) 982-0071

Attorneys for Plaintiff
MPH TECHNOLOGIES OY

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MPH TECHNOLOGIES OY,

Plaintiff,

v.

APPLE INC.,

Defendant.

Civil Action No. 3:18-cv-05935-TLT

Judge Trina L. Thompson

**PLAINTIFF'S PATENT L.R. 3.1
DISCLOSURE OF ASSERTED CLAIMS
AND INFRINGEMENT CONTENTIONS**

Plaintiff MPH Technologies Oy (“MPH”) hereby provides the following Disclosure of Asserted Claims and Infringement Contentions to Defendant Apple, Inc. (“Apple”) pursuant to Patent Local Rules 3-1 and 3-2.

These contentions are based on MPH’s current understanding of the claims of the asserted patents and information known to it at this time (May 15, 2023) without the benefit of information to be produced by Apple pursuant to MPH’s discovery requests served on May 1, 2023. MPH reserves all rights to supplement and/or amend its contentions pursuant to the Federal Rules of Civil Procedure, Orders of the Court, and Patent Local Rule 3-6, including based on any claim constructions by the Court that differ from those proposed by MPH and/or the discovery of nonpublic information regarding the accused instrumentalities.

I. Patent Local Rule 3-1 Disclosures

A. Identification of Infringed Claims of the Patents-In-Suit

Asserted Patent	Asserted Claims	Applicable Subsections of 35 U.S.C. § 271
U.S. Patent No. 8,346,949 B2 (“‘949 Patent”)	Claims 1, 3, 9, 11, 12, 13, and 28	35 U.S.C. § 271(a)
U.S. Patent No. 9,762,397 B2 (“‘397 Patent”)	Claim 1	35 U.S.C. § 271(a)
U.S. Patent No. 9,712,494 B2 (“‘494 Patent”)	Claims 2, 4, 9, and 11	35 U.S.C. § 271(a)
U.S. Patent No. 9,712,502 B2 (“‘502 Patent”)	Claims 7–9	35 U.S.C. § 271(a)-(c)
U.S. Patent No. 9,838,362 B2 (“‘362 Patent”)	Claims 3, 5, 10, 12-14, and 16	35 U.S.C. § 271(a)
U.S. Patent No. 7,937,581 B2 (“‘581 Patent”)	Claims 6–8	35 U.S.C. § 271(b)-(c)
U.S. Patent No. 8,037,302 B2 (“‘302 Patent”)	Claims 1–6, 9–11, 13, and 16	35 U.S.C. § 271(a)-(c)

B. Identification of Accused Instrumentalities

1. '949 Patent

The Apple devices that infringe the '949 Patent ("**Accused '949 Instrumentalities**") are the following Apple devices, servers, and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data:

- (a) Apple iOS devices that support and include iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, iOS 13, iOS 14, iOS 15, iOS 16, iPadOS 13, iPadOS 14, iPadOS 15, or iPadOS 16, including iPhone models 4S (A1431, A1387), 5 (A1428, A1429, A1442), 5C (A1456, A1507, A1516, A1529, A1532), 5S (A1453, A1457, A1518, A1528, A1530, A1533), 6 (A1549, A1586, A1589), 6 Plus (A1522, A1524, A1593), 6S (A1633, A1688, A1700), 6S Plus (A1634, A1687, A1699), SE (A1723, A1662, A1724), 7 (A1660, A1778), 7 Plus (A1661, A1784), 8 (A1863, A1905), 8Plus (A1864, A1897), X (A1865, A1901), XR (A1984, A2105, A2107), XS (A1920, A2097, A2099), XS Max (A1921, A2101, A2103), 11 (A2111), 11 Pro Max (A2161), 11 Pro (A2160), SE (2nd generation) (A2275), 12 mini (A2176), 12 (A2172), 12 Pro (A2341), 12 Pro Max (A2342), 13 mini (A2481), 13 (A2482), 13 Pro (A2483), 13 Pro Max (A2484), SE (3rd generation) (A2595), 14 (A2649), 14 Pro (A2650), 14 Pro Max (A2651), and iPhone 14 Plus (A2632); iPad models iPad 2 (A1395, A1397, A1396), iPad (2012) 3rd generation (A1416, A1430, A1403), iPad (2012) 4th generation (A1458, A1459, A1460), iPad (2017)/5th generation (A1822, A1823), iPad (2018)/6th generation (A1893, A1954), iPad 7th generation (A2197, A2200, A2198), iPad 8th generation (A2270, A2428, A2429, A2430), iPad 9th generation (A2602, A2603, A2604), iPad 10th Generation (A2696, A2757), iPad Air (A1474, A1475, A1476), iPad Air 2 (A1566, A1567), iPad Air 3rd generation (A2152, A2123, A2153), iPad Air 4th generation (A2316, A2324, A2325, A2072), iPad Air 5th generation (A2588, A2589, A2591), iPad Mini (A1432,

A1454, A1455), iPad Mini 2 (A1489, A1490, A1491), iPad Mini 3 (A1599, A1600), iPad Mini 4 (A1538, A1550), iPad Mini 5th generation (A2133, A2124, A2126), iPad Mini 6th generation (A2567, A2568), iPad Pro 9.7" (A1673, A1674, A1675), iPad Pro 10.5" (A1701, A1709), iPad Pro 12.9" (A1584, A1652), iPad Pro 12.9" 2nd generation (A1670, A1671), iPad Pro 11" (A1980, A2013, A1934), iPad Pro 12.9" 3rd generation (A1876, A2014, A1895), iPad Pro 11" 2nd generation (A2228, A2068, A2230), iPad Pro 12.9" 4th generation (A2229, A2069, A2232), iPad Pro 11" 3rd generation (A2377, A2459, A2301), iPad Pro 12.9" 5th generation (A2378, A2461, A2379), iPad Pro 11" 4th Generation (A2435, A2759, A2761), and iPad Pro 12.9" 6th Generation (A2436, A2437, A2764); iPod Touch 5th generation (A1509, A1421), iPod Touch 6th generation (A1574) and iPod Touch 7th generation (A2178);

(b) Apple macOS/OS X Products that support and include OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, macOS Catalina, macOS Big Sur, macOS Monterey, or macOS Ventura. The supported devices include MacBook (MacBook5,2 (MB881, MC240, A1278); MacBook6,1 (A1342); MacBook7,1 (A1342); MacBook8,1 (A1534); MacBook 9,1 (A1534); MacBook 10,1 (A1534)), MacBook Air (MacBookAir2,1 (A1304); MacBookAir3,1 (A1370); MacBookAir3,2 (A1369); MacBookAir4,1 (A1370); MacBookAir4,2 (A1369); MacBookAir5,1 (A1465); MacBookAir5,2 (A1466); MacBookAir6,1 (A1465); MacBookAir6,2 (A1466); MacBookAir7,1 (A1465); MacBookAir7,2 (A1466); MacBookAir8,1 (A1932); MacBookAir8,2 (A1932); MacBookAir9,1 (A2179); MacBookAir10,1 (A2337); Mac14,2 (A2681)), MacBook Pro (MacBookPro3,1 (A1226, A1229); MacBookPro4,1 (A1260, A1261); MacBookPro5,1 (A1286); MacBookPro5,2 (A1297); MacBookPro5,3 (A1286); MacBookPro5,5 (A1278); MacBookPro6,1 (A1297); MacBookPro6,2 (A1286); MacBookPro7,1 (A1278); MacBookPro8,1 (A1278); MacBookPro8,2 (A1286); MacBookPro8,3 (A1297); MacBookPro9,1 (A1286); MacBookPro9,2 (A1278); MacBookPro10,1 (A1398);

MacBookPro10,2 (A1425); MacBookPro11,1 (A1502); MacBookPro11,2 (A1398); MacBookPro11,3 (A1398); MacBookPro11,4 (A1502, A1398); MacBookPro11,5 (A1502, A1398); MacBookPro12,1 (A1502, A1398); MacBookPro13,1 (A1708); MacBookPro13,2 (A1706); MacBookPro13,3 (A1707); MacBookPro14,1 (A1708); MacBookPro14,2 (A1706); MacBookPro14,3 (A1707); MacBookPro15,1 (A1990); MacBookPro15,2 (A1989); MacBookPro15,3 (A1990); MacBookPro15,4 (A2159); MacBookPro16,1 (A2141); MacBookPro16,2 (A2251); MacBookPro16,3 (A2289); MacBookPro16,4 (A2141); MacBookPro17,1 (A2338); MacBookPro18,1 (A2485); MacBookPro18,2 (A2485); MacBookPro18,3 (A2442); MacBookPro18,4 (A2442); Mac14,7 (A2338); Mac14,5 (A2779); Mac14,6 (A2780); Mac14,9 (A2779); Mac14,10 (A2780)), Mac Mini (MacMini3,1 (A1283); MacMini4,1 (A1347); MacMini5,1 (A1347); MacMini5,2 (A1347); MacMini6,1 (A1347); MacMini6,2 (A1347); MacMini7,1 (A1347); MacMini8,1 (A1993); MacMini9,1 (A2348); Mac14,3 (A2686); Mac14,12 (A2816)), iMac (iMac7,1 (A1224, 1225); iMac8,1 (A1224, A1225); iMac9,1 (A1224, A1225); iMac10,1 (A1311, A1312); iMac11,1 (A1312); iMac11,2 (A1311); iMac11,3 (A1312); iMac12,1 (A2428, A2496); iMac12,2 (A2429); iMac13,1 (A1418); iMac13,2 (A1419); iMac14,1 (A1418); iMac14,2 (A1419); iMac14,3 (A1418); iMac14,4 (A1418); iMac15,1 (A1419); iMac16,1 (A1418); iMac16,2 (A1418); iMac17,1 (A1419); iMac18,1 (A1418); iMac18,2 (A1418); iMac18,3 (A1419); iMac19,1 (A2115); iMac19,2 (A2116); iMac20,1 (A2115); iMac20,2 (A2115); iMac21,1 (A2438); iMac21,2 (A2349)), Mac Pro (MacPro3,1 (A1186); MacPro4,1 (A1289); MacPro5,1 (A1289); MacPro6,1 (A1481); MacPro7,1 (A1991, A2304)), iMac Pro (iMacPro1,1 (A1862)), and Mac Studio (Mac13,1 (A2615); Mac13,2 (A2615));

(c) The Apple intermediate servers and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for

Apple Watch apps with streaming data. Based on presently available material, these servers include those supporting and enabling Apple's Push Notification service ("APNs"), which Apple's patent documentation describes as message servers. Based on Apple's publicly available documentation, other servers that support and enable the APNs include the Apple Identity Service ("IDS") servers.

(d) Apple Watches that support and include Watch OS 2.0, 3.0, 4.0, 5.0, 6.0, 7.0, 8.0 or 9.0 operating systems, namely, Apple Watch (1st generation) (A1553, A1554), Apple Watch Series 1 (A1802, A1803), Apple Watch Series 2 (A1757, A1758), Apple Watch Series 3 (A1858, A1859, A1860, A1861), Apple Watch Series 4 (A1977, A1978, A1975, A1976), Apple Watch Series 5 (A2092, A2093, A2094, A2095), Apple Watch SE (A2351, A2352, A2353, A2354), Apple Watch Series 6 (A2291, A2292, A2293, A2294), Apple Watch Series 7 (A2473, A2474, A2475, A2477), Apple Watch SE (2nd Generation) (A2722, A2723, A2726, A2727), Apple Watch Series 8 (A2770, A2771, A2772, A2774), and Apple Watch Ultra (A2622).

The Accused '949 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit A.

2. '397 Patent

The Apple devices that infringe the '397 Patent ("**Accused '397 Instrumentalities**") are the following Apple devices, servers, and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data:

(a) Apple iOS devices that support and include iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, iOS 13, iOS 14, iOS 15, iOS 16, iPadOS 13, iPadOS 14, iPadOS 15, or iPadOS 16, including iPhone models 4S (A1431, A1387), 5 (A1428, A1429, A1442), 5C (A1456, A1507, A1516, A1529, A1532), 5S (A1453, A1457, A1518, A1528, A1530, A1533), 6 (A1549, A1586, A1589), 6 Plus (A1522, A1524, A1593), 6S (A1633, A1688, A1700),

6S Plus (A1634, A1687, A1699), SE (A1723, A1662, A1724), 7 (A1660, A1778), 7 Plus (A1661, A1784), 8 (A1863, A1905), 8Plus (A1864, A1897), X (A1865, A1901), XR (A1984, A2105, A2107), XS (A1920, A2097, A2099), XS Max (A1921, A2101, A2103), 11 (A2111), 11 Pro Max (A2161), 11 Pro (A2160), SE (2nd generation) (A2275), 12 mini (A2176), 12 (A2172), 12 Pro (A2341), 12 Pro Max (A2342), 13 mini (A2481), 13 (A2482), 13 Pro (A2483), 13 Pro Max (A2484), SE (3rd generation) (A2595), 14 (A2649), 14 Pro (A2650), 14 Pro Max (A2651), and iPhone 14 Plus (A2632); iPad models iPad 2 (A1395, A1397, A1396), iPad (2012) 3rd generation (A1416, A1430, A1403), iPad (2012) 4th generation (A1458, A1459, A1460), iPad (2017)/5th generation (A1822, A1823), iPad (2018)/6th generation (A1893, A1954), iPad 7th generation (A2197, A2200, A2198), iPad 8th generation (A2270, A2428, A2429, A2430), iPad 9th generation (A2602, A2603, A2604), iPad 10th Generation (A2696, A2757), iPad Air (A1474, A1475, A1476), iPad Air 2 (A1566, A1567), iPad Air 3rd generation (A2152, A2123, A2153), iPad Air 4th generation (A2316, A2324, A2325, A2072), iPad Air 5th generation (A2588, A2589, A2591), iPad Mini (A1432, A1454, A1455), iPad Mini 2 (A1489, A1490, A1491), iPad Mini 3 (A1599, A1600), iPad Mini 4 (A1538, A1550), iPad Mini 5th generation (A2133, A2124, A2126), iPad Mini 6th generation (A2567, A2568), iPad Pro 9.7" (A1673, A1674, A1675), iPad Pro 10.5" (A1701, A1709), iPad Pro 12.9" (A1584, A1652), iPad Pro 12.9" 2nd generation (A1670, A1671), iPad Pro 11" (A1980, A2013, A1934), iPad Pro 12.9" 3rd generation (A1876, A2014, A1895), iPad Pro 11" 2nd generation (A2228, A2068, A2230), iPad Pro 12.9" 4th generation (A2229, A2069, A2232), iPad Pro 11" 3rd generation (A2377, A2459, A2301), iPad Pro 12.9" 5th generation (A2378, A2461, A2379), iPad Pro 11" 4th Generation (A2435, A2759, A2761), and iPad Pro 12.9" 6th Generation (A2436, A2437, A2764); iPod Touch 5th generation (A1509, A1421), iPod Touch 6th generation (A1574) and iPod Touch 7th generation (A2178);

(b) Apple macOS/OS X Products that support and include OS X Yosemite, OS X El

Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, macOS Catalina, macOS Big Sur, macOS Monterey, or macOS Ventura. The supported devices include MacBook (MacBook5,2 (MB881, MC240, A1278); MacBook6,1 (A1342); MacBook7,1 (A1342); MacBook8,1 (A1534); MacBook 9,1 (A1534); MacBook 10,1 (A1534)), MacBook Air (MacBookAir2,1 (A1304); MacBookAir3,1 (A1370); MacBookAir3,2 (A1369); MacBookAir4,1 (A1370); MacBookAir4,2 (A1369); MacBookAir5,1 (A1465); MacBookAir5,2 (A1466); MacBookAir6,1 (A1465); MacBookAir6,2 (A1466); MacBookAir7,1 (A1465); MacBookAir7,2 (A1466); MacBookAir8,1 (A1932); MacBookAir8,2 (A1932); MacBookAir9,1 (A2179); MacBookAir10,1 (A2337); Mac14,2 (A2681)), MacBook Pro (MacBookPro3,1 (A1226, A1229); MacBookPro4,1 (A1260, A1261); MacBookPro5,1 (A1286); MacBookPro5,2 (A1297); MacBookPro5,3 (A1286); MacBookPro5,5 (A1278); MacBookPro6,1 (A1297); MacBookPro6,2 (A1286); MacBookPro7,1 (A1278); MacBookPro8,1 (A1278); MacBookPro8,2 (A1286); MacBookPro8,3 (A1297); MacBookPro9,1 (A1286); MacBookPro9,2 (A1278); MacBookPro10,1 (A1398); MacBookPro10,2 (A1425); MacBookPro11,1 (A1502); MacBookPro11,2 (A1398); MacBookPro11,3 (A1398); MacBookPro11,4 (A1502, A1398); MacBookPro11,5 (A1502, A1398); MacBookPro12,1 (A1502, A1398); MacBookPro13,1 (A1708); MacBookPro13,2 (A1706); MacBookPro13,3 (A1707); MacBookPro14,1 (A1708); MacBookPro14,2 (A1706); MacBookPro14,3 (A1707); MacBookPro15,1 (A1990); MacBookPro15,2 (A1989); MacBookPro15,3 (A1990); MacBookPro15,4 (A2159); MacBookPro16,1 (A2141); MacBookPro16,2 (A2251); MacBookPro16,3 (A2289); MacBookPro16,4 (A2141); MacBookPro17,1 (A2338); MacBookPro18,1 (A2485); MacBookPro18,2 (A2485); MacBookPro18,3 (A2442); MacBookPro18,4 (A2442); Mac14,7 (A2338); Mac14,5 (A2779); Mac14,6 (A2780); Mac14,9(A2779); Mac14,10 (A2780)), Mac Mini (MacMini3,1 (A1283); MacMini4,1 (A1347); MacMini5,1 (A1347); MacMini5,2 (A1347); MacMini6,1 (A1347); MacMini6,2 (A1347);

MacMini7,1 (A1347); MacMini8,1 (A1993); MacMini9,1 (A2348); Mac14,3 (A2686); Mac14,12 (A2816)), iMac (iMac7,1 (A1224, 1225); iMac8,1 (A1224, A1225); iMac9,1 (A1224, A1225); iMac10,1 (A1311, A1312); iMac11,1 (A1312); iMac11,2 (A1311); iMac11,3 (A1312); iMac12,1 (A2428, A2496); iMac12,2 (A2429); iMac13,1 (A1418); iMac13,2 (A1419); iMac14,1 (A1418); iMac14,2 (A1419); iMac14,3 (A1418); iMac14,4 (A1418); iMac15,1 (A1419); iMac16,1 (A1418); iMac16,2 (A1418); iMac17,1 (A1419); iMac18,1 (A1418); iMac18,2 (A1418); iMac18,3 (A1419); iMac19,1 (A2115); iMac19,2 (A2116); iMac20,1 (A2115); iMac20,2 (A2115); iMac21,1 (A2438); iMac21,2 (A2349)), Mac Pro (MacPro3,1 (A1186); MacPro4,1 (A1289); MacPro5,1 (A1289); MacPro6,1 (A1481); MacPro7,1 (A1991, A2304)), iMac Pro (iMacPro1,1 (A1862)) and Mac Studio (Mac13,1 (A2615); Mac13,2 (A2615));

(c) The Apple intermediate servers and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data. Based on presently available material, these servers include those supporting and enabling Apple's Push Notification service ("APNs"), which Apple's patent documentation describes as message servers. Based on Apple's publicly available documentation, other servers that support and enable the APNs include the Apple Identity Service ("IDS") servers.

(d) Apple Watches that support and include Watch OS 2.0, 3.0, 4.0, 5.0, 6.0, 7.0, 8.0 or 9.0 operating systems, namely, Apple Watch (1st generation) (A1553, A1554), Apple Watch Series 1 (A1802, A1803), Apple Watch Series 2 (A1757, A1758), Apple Watch Series 3 (A1858, A1859, A1860, A1861), Apple Watch Series 4 (A1977, A1978, A1975, A1976), Apple Watch Series 5 (A2092, A2093, A2094, A2095), Apple Watch SE (A2351, A2352, A2353, A2354), Apple Watch Series 6 (A2291, A2292, A2293, A2294), Apple Watch Series 7 (A2473, A2474, A2475, A2477), Apple Watch SE (2nd

Generation) (A2722, A2723, A2726, A2727), Apple Watch Series 8 (A2770, A2771, A2772, A2774), and Apple Watch Ultra (A2622).

The Accused '397 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit B.

3. '494 Patent

The Apple devices that infringe the '494 Patent ("Accused '494 Instrumentalities") are the Apple servers and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data. Based on presently available material, these servers include those supporting and enabling Apple's Push Notification service ("APNs"), which Apple's patent documentation describes as message servers. Based on Apple's publicly available documentation, other servers that support and enable the APNs include the Apple Identity Service ("IDS") servers.

The Accused '494 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit C.

4. '502 Patent

The Apple devices that infringe the '502 Patent ("**Accused '502 Instrumentalities**") are the following Apple devices and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data:

- (a) Apple iOS devices that support and include iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, iOS 13, iOS 14, iOS 15, iOS 16, iPadOS 13, iPadOS 14, iPadOS 15, or iPadOS 16, including iPhone models 4S (A1431, A1387), 5 (A1428, A1429, A1442), 5C (A1456, A1507, A1516, A1529, A1532), 5S (A1453, A1457, A1518, A1528, A1530, A1533), 6 (A1549, A1586, A1589), 6 Plus (A1522, A1524, A1593), 6S (A1633, A1688, A1700), 6S Plus (A1634, A1687, A1699), SE (A1723, A1662, A1724), 7 (A1660, A1778), 7 Plus (A1661, A1784), 8 (A1863, A1905), 8Plus (A1864, A1897), X (A1865,

1 A1901), XR (A1984, A2105, A2107), XS (A1920, A2097, A2099), XS Max (A1921,
 2 A2101, A2103), 11 (A2111), 11 Pro Max (A2161), 11 Pro (A2160), SE (2nd generation)
 3 (A2275), 12 mini (A2176), 12 (A2172), 12 Pro (A2341), 12 Pro Max (A2342), 13 mini
 4 (A2481), 13 (A2482), 13 Pro (A2483), 13 Pro Max (A2484), SE (3rd generation)
 5 (A2595), 14 (A2649), 14 Pro (A2650), 14 Pro Max (A2651), and iPhone 14 Plus
 6 (A2632); iPad models iPad 2 (A1395, A1397, A1396), iPad (2012) 3rd generation
 7 (A1416, A1430, A1403), iPad (2012) 4th generation (A1458, A1459, A1460), iPad
 8 (2017)/5th generation (A1822, A1823), iPad (2018)/6th generation (A1893, A1954),
 9 iPad 7th generation (A2197, A2200, A2198), iPad 8th generation (A2270, A2428,
 10 A2429, A2430), iPad 9th generation (A2602, A2603, A2604), iPad 10th generation
 11 (A2696, A2757), iPad Air (A1474, A1475, A1476), iPad Air 2 (A1566, A1567), iPad
 12 Air 3rd generation (A2152, A2123, A2153), iPad Air 4th generation (A2316, A2324,
 13 A2325, A2072), iPad Air 5th generation (A2588, A2589, A2591), iPad Mini (A1432,
 14 A1454, A1455), iPad Mini 2 (A1489, A1490, A1491), iPad Mini 3 (A1599, A1600),
 15 iPad Mini 4 (A1538, A1550), iPad Mini 5th generation (A2133, A2124, A2126), iPad
 16 Mini 6th generation (A2567, A2568), iPad Pro 9.7" (A1673, A1674, A1675), iPad Pro
 17 10.5" (A1701, A1709), iPad Pro 12.9" (A1584, A1652), iPad Pro 12.9" 2nd generation
 18 (A1670, A1671), iPad Pro 11" (A1980, A2013, A1934), iPad Pro 12.9" 3rd generation
 19 (A1876, A2014, A1895), iPad Pro 11" 2nd generation (A2228, A2068, A2230), iPad
 20 Pro 12.9" 4th generation (A2229, A2069, A2232), iPad Pro 11" 3rd generation (A2377,
 21 A2459, A2301), iPad Pro 12.9" 5th generation (A2378, A2461, A2379), iPad Pro 11"
 22 4th Generation (A2435, A2759, A2761), and iPad Pro 12.9" 6th Generation (A2436,
 23 A2437, A2764); iPod Touch 5th generation (A1509, A1421), iPod Touch 6th generation
 24 (A1574) and iPod Touch 7th generation (A2178);

25 (b) Apple macOS/OS X Products that support and include OS X Yosemite, OS X El
 26 Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, macOS Catalina, macOS
 27 Big Sur, macOS Monterey, or macOS Ventura. The supported devices include

MacBook (MacBook5,2 (MB881, MC240, A1278); MacBook6,1 (A1342);
 MacBook7,1 (A1342); MacBook8,1 (A1534); MacBook 9,1 (A1534); MacBook 10,1
 (A1534)), MacBook Air (MacBookAir2,1 (A1304); MacBookAir3,1 (A1370);
 MacBookAir3,2 (A1369); MacBookAir4,1 (A1370); MacBookAir4,2 (A1369);
 MacBookAir5,1 (A1465); MacBookAir5,2 (A1466); MacBookAir6,1 (A1465);
 MacBookAir6,2 (A1466); MacBookAir7,1 (A1465); MacBookAir7,2 (A1466);
 MacBookAir8,1 (A1932); MacBookAir8,2 (A1932); MacBookAir9,1 (A2179);
 MacBookAir10,1 (A2337); Mac14,2 (A2681)), MacBook Pro (MacBookPro3,1
 (A1226, A1229); MacBookPro4,1 (A1260, A1261); MacBookPro5,1 (A1286);
 MacBookPro5,2 (A1297); MacBookPro5,3 (A1286); MacBookPro5,5 (A1278);
 MacBookPro6,1 (A1297); MacBookPro6,2 (A1286); MacBookPro7,1 (A1278);
 MacBookPro8,1 (A1278); MacBookPro8,2 (A1286); MacBookPro8,3 (A1297);
 MacBookPro9,1 (A1286); MacBookPro9,2 (A1278); MacBookPro10,1 (A1398);
 MacBookPro10,2 (A1425); MacBookPro11,1 (A1502); MacBookPro11,2 (A1398);
 MacBookPro11,3 (A1398); MacBookPro11,4 (A1502, A1398); MacBookPro11,5
 (A1502, A1398); MacBookPro12,1 (A1502, A1398); MacBookPro13,1 (A1708);
 MacBookPro13,2 (A1706); MacBookPro13,3 (A1707); MacBookPro14,1 (A1708);
 MacBookPro14,2 (A1706); MacBookPro14,3 (A1707); MacBookPro15,1 (A1990);
 MacBookPro15,2 (A1989); MacBookPro15,3 (A1990); MacBookPro15,4 (A2159);
 MacBookPro16,1 (A2141); MacBookPro16,2 (A2251); MacBookPro16,3 (A2289);
 MacBookPro16,4 (A2141); MacBookPro17,1 (A2338); MacBookPro18,1 (A2485);
 MacBookPro18,2 (A2485); MacBookPro18,3 (A2442); MacBookPro18,4 (A2442);
 Mac14,7 (A2338); Mac14,5 (A2779); Mac14,6 (A2780); Mac14,9 (A2779); Mac14,10
 (A2780)), Mac Mini (MacMini3,1 (A1283); MacMini4,1 (A1347); MacMini5,1
 (A1347); MacMini5,2 (A1347); MacMini6,1 (A1347); MacMini6,2 (A1347);
 MacMini7,1 (A1347); MacMini8,1 (A1993); MacMini9,1 (A2348); Mac14,3 (A2686);
 Mac14,12 (A2816)), iMac (iMac7,1 (A1224, 1225); iMac8,1 (A1224, A1225);

iMac9,1 (A1224, A1225), iMac10,1 (A1311, A1312); iMac11,1 (A1312); iMac11,2 (A1311); iMac11,3 (A1312); iMac12,1 (A2428, A2496); iMac12,2 (A2429); iMac13,1 (A1418); iMac13,2 (A1419); iMac14,1 (A1418); iMac14,2 (A1419); iMac14,3 (A1418); iMac14,4 (A1418); iMac15,1 (A1419); iMac16,1 (A1418); iMac16,2 (A1418); iMac17,1 (A1419); iMac18,1 (A1418); iMac18,2 (A1418); iMac18,3 (A1419); iMac19,1 (A2115); iMac19,2 (A2116); iMac20,1 (A2115); iMac20,2 (A2115); iMac21,1 (A2438); iMac21,2 (A2349)), Mac Pro (MacPro3,1 (A1186); MacPro4,1 (A1289); MacPro5,1 (A1289); MacPro6,1 (A1481); MacPro7,1 (A1991, A2304)), iMac Pro (iMacPro1,1 (A1862)) and Mac Studio (Mac13,1 (A2615); Mac13,2 (A2615));

(c) Apple Watches that support and include Watch OS 2.0, 3.0, 4.0, 5.0, 6.0, 7.0, 8.0, or 9.0 operating systems, namely, Apple Watch (1st generation) (A1553, A1554), Apple Watch Series 1 (A1802, A1803), Apple Watch Series 2 (A1757, A1758), Apple Watch Series 3 (A1858, A1859, A1860, A1861), Apple Watch Series 4 (A1977, A1978, A1975, A1976), Apple Watch Series 5 (A2092, A2093, A2094, A2095), Apple Watch SE (A2351, A2352, A2353, A2354), Apple Watch Series 6 (A2291, A2292, A2293, A2294), Apple Watch Series 7 (A2473, A2474, A2475, A2477) Apple Watch SE (2nd Generation) (A2722, A2723, A2726, A2727), Apple Watch Series 8 (A2770, A2771, A2772, A2774), and Apple Watch Ultra (A2622).

The Accused '502 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit D.

5. '362 Patent

The Apple devices that infringe the '362 Patent ("Accused '362 Instrumentalities") are the Apple servers and associated software that support and enable Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data. Based on presently available material, these servers include those supporting and enabling Apple's Push

Notification service (“APNs”), which Apple’s patent documentation describes as message servers. Based on Apple’s publicly available documentation, other servers that support and enable the APNs include the Apple Identity Service (“IDS”) servers. The Accused ’362 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit E.

6. ’581 Patent

The Apple devices that infringe the ’581 Patent (“Accused ’581 Instrumentalities”) are the following Apple products that provide IKEv2 type VPN and enable MOBIKE (RFC 4555):

- (a) Apple iOS devices that support and include iOS 9, iOS 10, iOS 11, iOS 12, iOS 13, iOS 14, iOS 15, iOS 16, iPadOS 13, iPadOS 14, iPadOS 15, or iPadOS 16, including iPhone models 4S (A1431, A1387), 5 (A1428, A1429, A1442), 5C (A1456, A1507, A1516, A1529, A1532), 5S (A1453, A1457, A1518, A1528, A1530, A1533), 6 (A1549, A1586, A1589), 6 Plus (A1522, A1524, A1593), 6S (A1633, A1688, A1700), 6S Plus (A1634, A1687, A1699), SE (A1723, A1662, A1724), 7 (A1660, A1778), 7 Plus (A1661, A1784), 8 (A1863, A1905), 8Plus (A1864, A1897), X (A1865, A1901), XR (A1984, A2105, A2107), XS (A1920, A2097, A2099), XS Max (A1921, A2101, A2103), 11 (A2111), 11 Pro Max (A2161), 11 Pro (A2160), SE (2nd generation) (A2275), 12 mini (A2176), 12 (A2172), 12 Pro (A2341), 12 Pro Max (A2342), 13 mini (A2481), 13 (A2482), 13 Pro (A2483), 13 Pro Max (A2484), SE (3rd generation) (A2595), 14 (A2649), 14 Pro (A2650), 14 Pro Max (A2651); iPad models iPad 2 (A1395, A1397, A1396), iPad (2012) 3rd generation (A1416, A1430, A1403), iPad (2012) 4th generation (A1458, A1459, A1460), iPad (2017)/5th generation (A1822, A1823), iPad (2018)/6th generation (A1893, A1954), iPad 7th generation (A2197, A2200, A2198), iPad 8th generation (A2270, A2428, A2429, A2430), iPad 9th generation (A2602, A2603, A2604), iPad Air (A1474, A1475, A1476), iPad Air 2 (A1566, A1567), iPad Air 3rd generation (A2152, A2123, A2153), iPad Air 4th generation (A2316, A2324, A2325, A2072), iPad Air 5th generation (A2588, A2589, A2591), iPad Mini (A1432, A1454, A1455), iPad Mini 2 (A1489, A1490, A1491), iPad

1 Mini 3 (A1599, A1600), iPad Mini 4 (A1538, A1550), iPad Mini 5th generation
 2 (A2133, A2124, A2126), iPad Mini 6th generation (A2567, A2568), iPad Pro 9.7”
 3 (A1673, A1674, A1675), iPad Pro 10.5” (A1701, A1709), iPad Pro 12.9” (A1584,
 4 A1652), iPad Pro 12.9” 2nd generation (A1670, A1671), iPad Pro 11” (A1980, A2013,
 5 A1934), iPad Pro 12.9” 3rd generation (A1876, A2014, A1895), iPad Pro 11” 2nd
 6 generation (A2228, A2068, A2230), iPad Pro 12.9” 4th generation (A2229, A2069,
 7 A2232), iPad Pro 11” 3rd generation (A2377, A2459, A2301), iPad Pro 12.9” 5th
 8 generation (A2378, A2461, A2379); iPod Touch 5th generation (A1509, A1421), iPod
 9 Touch 6th generation (A1574) and iPod Touch 7th generation (A2178); and
 10 (b) Apple macOS/OS X Products that support and include OS X El Capitan, macOS
 11 Sierra, macOS High Sierra, macOS Mojave, macOS Catalina, macOS Big Sur, macOS
 12 Monterey, or macOS Ventura. The supported devices include MacBook (MacBook5,2
 13 (MB881, MC240, A1278); MacBook6,1 (A1342); MacBook7,1 (A1342);
 14 MacBook8,1 (A1534); MacBook 9,1 (A1534); MacBook 10,1 (A1534)), MacBook Air
 15 (MacBookAir2,1 (A1304); MacBookAir3,1 (A1370); MacBookAir3,2 (A1369);
 16 MacBookAir4,1 (A1370); MacBookAir4,2 (A1369); MacBookAir5,1 (A1465);
 17 MacBookAir5,2 (A1466); MacBookAir6,1 (A1465); MacBookAir6,2 (A1466);
 18 MacBookAir7,1 (A1465); MacBookAir7,2 (A1466); MacBookAir8,1 (A1932);
 19 MacBookAir8,2 (A1932); MacBookAir9,1 (A2179); MacBookAir10,1 (A2337);
 20 Mac14,2 (A2681)), MacBook Pro (MacBookPro3,1 (A1226, A1229); MacBookPro4,1
 21 (A1260, A1261); MacBookPro5,1 (A1286); MacBookPro5,2 (A1297);
 22 MacBookPro5,3 (A1286); MacBookPro5,5 (A1278); MacBookPro6,1 (A1297);
 23 MacBookPro6,2 (A1286); MacBookPro7,1 (A1278); MacBookPro8,1 (A1278);
 24 MacBookPro8,2 (A1286); MacBookPro8,3 (A1297); MacBookPro9,1 (A1286);
 25 MacBookPro9,2 (A1278); MacBookPro10,1 (A1398); MacBookPro10,2 (A1425);
 26 MacBookPro11,1 (A1502); MacBookPro11,2 (A1398); MacBookPro11,3 (A1398);
 27 MacBookPro11,4 (A1502, A1398); MacBookPro11,5 (A1502, A1398);

MacBookPro12,1 (A1502, A1398); MacBookPro13,1 (A1708); MacBookPro13,2 (A1706); MacBookPro13,3 (A1707); MacBookPro14,1 (A1708); MacBookPro14,2 (A1706); MacBookPro14,3 (A1707); MacBookPro15,1 (A1990); MacBookPro15,2 (A1989); MacBookPro15,3 (A1990); MacBookPro15,4 (A2159); MacBookPro16,1 (A2141); MacBookPro16,2 (A2251); MacBookPro16,3 (A2289); MacBookPro16,4 (A2141); MacBookPro17,1 (A2338); MacBookPro18,1 (A2485); MacBookPro18,2 (A2485); MacBookPro18,3 (A2442); MacBookPro18,4 (A2442); Mac14,7 (A2338)), Mac Mini (MacMini3,1 (A1283); MacMini4,1 (A1347); MacMini5,1 (A1347); MacMini5,2 (A1347); MacMini6,1 (A1347); MacMini6,2 (A1347); MacMini7,1 (A1347); MacMini8,1 (A1993); MacMini9,1 (A2348)), iMac (iMac7,1 (A1224, 1225); iMac8,1 (A1224, A1225); iMac9,1 (A1224, A1225); iMac10,1 (A1311, A1312); iMac11,1 (A1312); iMac11,2 (A1311); iMac11,3 (A1312); iMac12,1 (A2428, A2496); iMac12,2 (A2429); iMac13,1 (A1418); iMac13,2 (A1419); iMac14,1 (A1418); iMac14,2 (A1419); iMac14,3 (A1418); iMac14,4 (A1418); iMac15,1 (A1419); iMac16,1 (A1418); iMac16,2 (A1418); iMac17,1 (A1419); iMac18,1 (A1418); iMac18,2 (A1418); iMac18,3 (A1419); iMac19,1 (A2115); iMac19,2 (A2116); iMac20,1 (A2115); iMac20,2 (A2115); iMac21,1 (A2438); iMac21,2 (A2349)), Mac Pro (MacPro3,1 (A1186); MacPro4,1 (A1289); MacPro5,1 (A1289); MacPro6,1 (A1481); MacPro7,1 (A1991, A2304)), iMac Pro (iMacPro1,1 (A1862)), and Mac Studio (Mac13,1 (A2615); Mac13,2 (A2615)).

The Accused '581 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit F.

7. '302 Patent

The Apple devices and associated software that infringe the '302 Patent ("**Accused '302 Instrumentalities**") are the following Apple devices and associated software that utilize and enable Apple Always On VPN when used with VPN gateways and VPN servers:

Apple iOS devices that support and include iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, iOS 13, iOS 14, iOS 15, iOS 16, iPadOS 13, iPadOS 14, iPadOS 15, or iPadOS 16, including iPhone models 4S (A1431, A1387), 5 (A1428, A1429, A1442), 5C (A1456, A1507, A1516, A1529, A1532), 5S (A1453, A1457, A1518, A1528, A1530, A1533), 6 (A1549, A1586, A1589), 6 Plus (A1522, A1524, A1593), 6S (A1633, A1688, A1700), 6S Plus (A1634, A1687, A1699), SE (A1723, A1662, A1724), 7 (A1660, A1778), 7 Plus (A1661, A1784), 8 (A1863, A1905), 8Plus (A1864, A1897), X (A1865, A1901), XR (A1984, A2105, A2107), XS (A1920, A2097, A2099), XS Max (A1921, A2101, A2103), 11 (A2111), 11 Pro Max (A2161), 11 Pro (A2160), SE (2nd generation) (A2275), 12 mini (A2176), 12 (A2172), 12 Pro (A2341), 12 Pro Max (A2342), 13 mini (A2481), 13 (A2482), 13 Pro (A2483), 13 Pro Max (A2484), SE (3rd generation) (A2595), 14 (A2649), 14 Pro (A2650), 14 Pro Max (A2651), and iPhone 14 Plus (A2632); iPad models iPad 2 (A1397, 1396), iPad (2012) 3rd generation (A1430, A1403), iPad (2012) 4th generation (A1459, A1460), iPad (2017)/5th generation (A1823), iPad (2018)/6th generation (A1954), iPad 7th generation (A2200, A2198), iPad 8th generation (A2428, A2429, A2430), iPad 9th generation (A2603, A2604), iPad 10th Generation (A2757), iPad Air (A1475, A1476), iPad Air 2 (A1567), iPad Air 3rd generation (A2123, A2153), iPad Air 4th generation (A2324, A2325, A2072), iPad Air 5th generation (A2589, A2591), iPad Mini (A1454, A1455), iPad Mini 2 (A1490, A1491), iPad Mini 3 (A1600), iPad Mini 4 (A1550), iPad Mini 5th generation (A2124, A2126), iPad Mini 6th generation (A2568), iPad Pro 9.7" (A1674, A1675), iPad Pro 10.5" (A1709), iPad Pro 12.9" (A1652), iPad Pro 12.9" 2nd generation (A1671), iPad Pro 11" (A2013, A1934), iPad Pro 12.9" 3rd generation (A2014, A1895), iPad Pro 11" 2nd generation (A2068, A2230), iPad Pro 12.9" 4th generation (A2069, A2232), iPad Pro 11" 3rd generation (A2459, A2301), iPad Pro 12.9" 5th generation (A2461, A2379), iPad Pro 11" 4th Generation (A2435, A2759, A2761), and iPad Pro 12.9" 6th Generation (A2436, A2437, A2764).

The Accused '302 Instrumentalities have also been identified in the corresponding claim chart, which is attached hereto as Exhibit G.

C. Claim Charts

Charts applying the asserted claims to the Accused Instrumentalities are attached as Exhibits A-G as follows:

Exhibit	Asserted Patent
Exhibit A	'949 Patent
Exhibit B	'397 Patent
Exhibit C	'494 Patent
Exhibit D	'502 Patent
Exhibit E	'362 Patent
Exhibit F	'581 Patent
Exhibit G	'302 Patent

MPH does not contend that any terms are governed by 35 U.S.C. § 112(6).

D. Indirect Infringement and Direct Infringement Based on Multiple Parties

1. '949 Patent – Direct infringement based on joint acts of multiple parties

In addition to infringing the '949 Patent directly based entirely on Apple's own acts, including Apple testing its products and otherwise executing the claimed methods in the course of product development and support, Apple has and continues to directly infringe the '949 Patent based on joint acts of multiple parties. Specifically, Apple has infringed and continues to infringe at least claims 1, 3, 9, 11, 12, 13, and 28 of the '949 Patent under 35 U.S.C. § 271(a) by making, using, and operating within the United States the Accused '949 Instrumentalities that support and enable its iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data, which also use the Apple Push Notification service ("APNs") and Apple Identity

1 service (“IDS”) to support end-to-end encryption, as well as by directing and controlling, and
 2 conditioning its customers’ and end users’ participation and use of, and receipt of the benefits of,
 3 iMessage, FaceTime, Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text
 4 Message Forwarding, and encryption for Apple Watch apps with streaming data, upon the
 5 performance of steps of claims 1, 3, 9, 11, 12, 13, and 28 of the ’949 Patent and establishing the
 6 manner and timing of that performance. See attached claim chart.

7 Apple maintains absolute control over the operation of its iMessage and FaceTime services,
 8 as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message
 9 Forwarding, and encryption for Apple Watch apps with streaming data, including its operation of
 10 the software, servers, and databases that support such services. Users are required to sign up and
 11 agree to numerous terms and conditions unilaterally imposed by Apple, including in its user
 12 software licenses, account agreements (iTunes/Apple ID), and privacy agreements, in order to use
 13 them.

14 Apple begins its “iOS Software License Agreement” by stating that “BY USING YOUR
 15 IPHONE, IPAD or IPOD Touch (“iOS DEVICE”), YOU ARE AGREEING TO BE BOUND BY
 16 THE FOLLOWING TERMS.” See “Apple Inc. iOS Software License Agreement”
 17 (www.apple.com/legal/sla/docs/iOS112.pdf); *see also* Apple Inc. Software License Agreement for
 18 macOS High Sierra (www.apple.com/legal/sla/docs/macOS1013.pdf); *see also* iOS16 and
 19 iPadOS16 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS15 and iPadOS15
 20 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS14 and iPadOS14 “Apple Inc.
 21 iOS and iPadOS Software License Agreement”; iOS13 and iPadOS13 “Apple Inc. iOS and
 22 iPadOS Software License Agreement”; iOS12 “Apple Inc. iOS Software License Agreement”;
 23 iOS10 “Apple Inc. iOS Software License Agreement”; iOS 9 “Apple Inc. iOS Software License
 24 Agreement”; iOS 8 “Apple Inc. iOS Software License Agreement;” “Apple Inc. Software License
 25 Agreement for macOS Ventura”; “Apple Inc. Software License Agreement for macOS Monterey;”
 26 “Apple Inc. Software License Agreement for macOS Big Sur;” “Apple Inc. Software License
 27 Agreement for macOS Catalina;” “Apple Inc. Software License Agreement for macOS Mojave;”

1 “Apple Inc. Software License Agreement for macOS Sierra;” “Apple Inc. Software License
 2 Agreement for macOS El Capitan;” “Apple Inc. Software License Agreement for macOS
 3 Yosemite;” Apple watchOS Software License Agreement, all available at
 4 <https://www.apple.com/legal/sla/>.

5 The Apple iOS Software License Agreement, to which each Apple iOS device user wishing
 6 to have access to, receive the benefit of, and use iMessage and FaceTime must agree, also provides:

7 The software (including Boot ROM code, embedded software and third party
 8 software), documentation, interfaces, content, fonts and any data that came with
 9 your iOS Device (“Original iOS Software”), as may be updated or replaced by
 10 feature enhancements, software updates or system restore software provided by
 11 Apple (“iOS Software Updates”), whether in read only memory, on any other media
 12 or in any other form (the Original iOS Software and iOS Software Updates are
 13 collectively referred to as the “iOS Software”) are licensed, not sold, to you by
 14 Apple Inc. (“Apple”) for use only under the terms of this License. Apple and its
 licensors retain ownership of the iOS Software itself and reserve all rights not
 expressly granted to you. You agree that the terms of this License will apply to any
 Apple-branded app that may be built-in on your iOS Device, unless such app is
 accompanied by a separate license, in which case you agree that the terms of that
 license will govern your use of that app.

15 See “Apple Inc. iOS Software License Agreement” (www.apple.com/legal/sla/docs/iOS112.pdf);
 16 See also iOS16 and iPadOS16 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS15
 17 and iPadOS15 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS14 and iPadOS14
 18 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS13 and iPadOS13 “Apple Inc.
 19 iOS and iPadOS Software License Agreement”; iOS12 “Apple Inc. iOS Software License
 20 Agreement”; iOS11 “Apple Inc. iOS Software License Agreement”; iOS10 “Apple Inc. iOS
 21 Software License Agreement”; iOS 9 “Apple Inc. iOS Software License Agreement”; iOS 8
 22 “Apple Inc. iOS Software License Agreement”; Apple watchOS Software License Agreement, all
 23 available at <https://www.apple.com/legal/sla/>.

24 Similarly, the Apple macOS software license agreement states:

25 The Apple software (including Boot ROM code), any third party software,
 26 documentation, interfaces, content, fonts and any data accompanying this License
 27 whether preinstalled on Apple-branded hardware, on disk, in read only memory, on
 any other media or in any other form (collectively the “Apple Software”) are
 licensed, not sold, to you by Apple Inc. (“Apple”) for use only under the terms of

1 this License. Apple and/or Apple's licensors retain ownership of the Apple
 2 Software itself and reserve all rights not expressly granted to you. You agree that
 3 the terms of this License will apply to any Apple-branded application software
 4 product that may be preinstalled on your Apple-branded hardware, unless such
 product is accompanied by a separate license, in which case you agree that the terms
 of that license will govern your use of that product.

5 *See also* Apple Inc. Software License Agreement for macOS High Sierra
 6 (www.apple.com/legal/sla/docs/macOS1013.pdf); "Apple Inc. Software License Agreement for
 7 macOS Ventura"; "Apple Inc. Software License Agreement for macOS Monterey;" "Apple Inc.
 8 Software License Agreement for macOS Big Sur;" "Apple Inc. Software License Agreement for
 9 macOS Catalina;" "Apple Inc. Software License Agreement for macOS Mojave;" "Apple Inc.
 10 Software License Agreement for macOS Sierra;" "Apple Inc. Software License Agreement for
 11 macOS El Capitan;" "Apple Inc. Software License Agreement for macOS Yosemite;" all available
 12 at <https://www.apple.com/legal/sla/>.

13 Additionally, Apple requires each user of iMessage and FaceTime to register and obtain
 14 an Apple ID as a prerequisite to using these services. Prior to using the services, each user must
 15 first log in and then provide and allow Apple to access, store, and use the user's unique identifier.
 16 These requirements are set forth in Apple's software license agreements for both iOS and macOS:

17 Use of the App Store requires a unique user name and password combination,
 18 known as an Apple ID. An Apple ID is also required to access app updates and
 certain features of the iOS Software and Services.

* * *

19 Consent to Use of Data. When you use your device, your phone number and certain
 20 unique identifiers for your iOS Device are sent to Apple in order to allow others to
 21 reach you by your phone number when using various communication features of
 22 the iOS Software, such as iMessage and FaceTime. When you use iMessage, Apple
 may hold your messages in encrypted form for a limited period of time in order to
 ensure their delivery.

* * *

23 By using this software in connection with an Apple ID, or other Apple Service, you
 24 agree to the applicable terms of service for that Service, such as the latest Apple
 25 Media Services Terms and Conditions for the country in which you access such
 26 Services, which you may access and review at
<http://www.apple.com/legal/internet-services/itunes/ww/>.

1 “Apple Inc. iOS Software License Agreement” (www.apple.com/legal/sla/docs/iOS112.pdf); *see*
 2 *also* Apple Inc. Software License Agreement for macOS High Sierra
 3 (www.apple.com/legal/sla/docs/macOS1013.pdf); iOS16 and iPadOS16 “Apple Inc. iOS and
 4 iPadOS Software License Agreement”; iOS15 and iPadOS15 “Apple Inc. iOS and iPadOS
 5 Software License Agreement”; iOS14 and iPadOS14 “Apple Inc. iOS and iPadOS Software
 6 License Agreement”; iOS13 and iPadOS13 “Apple Inc. iOS and iPadOS Software License
 7 Agreement”; iOS12 “Apple Inc. iOS Software License Agreement”; iOS10 “Apple Inc. iOS
 8 Software License Agreement”; iOS 9 “Apple Inc. iOS Software License Agreement”; iOS 8
 9 “Apple Inc. iOS Software License Agreement;” “Apple Inc. Software License Agreement for
 10 macOS Ventura;” “Apple Inc. Software License Agreement for macOS Monterey;” “Apple Inc.
 11 Software License Agreement for macOS Big Sur;” “Apple Inc. Software License Agreement for
 12 macOS Catalina;” “Apple Inc. Software License Agreement for macOS Mojave;” “Apple Inc.
 13 Software License Agreement for macOS Sierra;” “Apple Inc. Software License Agreement for
 14 macOS El Capitan;” “Apple Inc. Software License Agreement for macOS Yosemite;” all available
 15 at <https://www.apple.com/legal/sla/>.

16 Apple further requires end users to provide personal information and other identifying
 17 information to access services provided by Apple, including the iMessage and FaceTime services,
 18 and to receive benefits from such services:

19 Personal information is data that can be used to identify or contact a single person.
 20 You may be asked to provide your personal information anytime you are in contact
 21 with Apple or an Apple affiliated company. Apple and its affiliates may share this
 22 personal information with each other and use it consistent with this Privacy Policy.
 23 They may also combine it with other information to provide and improve our
 24 products, services, content, and advertising. You are not required to provide the
 25 personal information that we have requested, but, if you chose not to do so, in many
 26 cases we will not be able to provide you with our products or services or respond
 27 to any queries you may have.

28 * * *

25 We may collect information such as occupation, language, zip code, area code,
 26 unique device identifier, referrer URL, location, and the time zone where an Apple
 27 product is used so that we can better understand customer behavior and improve
 28 our products, services, and advertising.

1 <https://www.apple.com/privacy/privacy-policy/> (accessed in 2018); *see also* Messages & Privacy,
2 available at <https://www.apple.com/legal/privacy/data/en/messages/>; FaceTime & Privacy,
3 available at <https://www.apple.com/legal/privacy/data/en/face-time/>.

4 Based on at least the above facts, Apple directs or controls the performance of end users of
5 its devices operating Apple's iMessage and FaceTime services. Apple has the right and ability to
6 stop or limit use of its iMessage and FaceTime services. Apple conditions use of Apple devices
7 and software, including use of the iMessage and FaceTime services and the benefits derived
8 therefrom, upon agreeing to the above legal terms, including performance of the relevant acts of
9 infringement carried out by its devices for which Apple establishes the manner and timing of such
10 performance as set forth below.

11 The Apple iMessage and FaceTime services enable the end user Accused '949
12 Instrumentalities including iPhones, iPads, iPods, Apple Watches, Mac computers, when operated
13 by customers and end users, to send and receive secure messages over a telecommunications
14 network, i.e., the Internet, via the server Accused '949 Instrumentalities, including the APNs and
15 IDS servers operated by Apple. In its Answer, Apple has denied that it owns and operates the
16 APNs servers. (*See* Dkt. No. 38 at ¶56). MPH intends to seek discovery on the basis for Apple's
17 denial. To the extent Apple contracts with third parties who own or operate the servers which
18 perform the salient functionality, such operation is attributable to Apple.

19 More specifically, when operated as intended and required by Apple and under Apple's
20 direction and control, pursuant to Apple's software licenses, privacy policies, and other user
21 agreements, Apple end user devices, including iPhones, iPads, iPods, Apple Watches, and Mac
22 computers, establish a secure connection with one another by negotiating and exchanging keys
23 with one another according to a key exchange protocol through intermediate Apple servers
24 operated by Apple. Each Apple end user device is configured to be assigned with an IP address,
25 which may change, including when the connection is changed from a cellular network to a Wi-Fi
26 network.

27 When operated as intended and required by Apple and under Apple's direction and control,

1 pursuant to Apple's software licenses, privacy policies, and other user agreements, Apple end user
2 devices are configured to form secure messages using the functionalities of iMessage and
3 FaceTime. Messages sent through iMessage and FaceTime include a device token, which is a
4 unique identifier assigned by Apple that identifies a unique app-device combination, which is used
5 to forward messages to receiving Apple end user devices. Messages formed by Apple end user
6 devices also include an address of Apple servers, including Apple's APNs servers. Such messages
7 include payloads encrypted using encryption keys from a key exchange protocol.

8 Intermediate Apple servers, including Apple's APNs servers operated by Apple, receive
9 encrypted message payloads sent by Apple end user devices to provide the iMessage and FaceTime
10 services. Apple servers, including its APNs servers, decrypt device tokens and use such tokens to
11 locate the addresses of the intended recipients of encrypted message payloads. The decrypted
12 tokens are included with the encrypted message payloads, thus replacing the encrypted device
13 tokens. Apple is unable to decrypt the payloads of the messages. Apple's APNs servers map device
14 tokens with connections to receiving devices. Apple utilizes a table located at Apple's APNs
15 servers to map a device token to connection information of the receiving device. Apple utilizes a
16 table located at Apple's APNs servers to map a device token to connection information of the
17 receiving device including the receiving device's location or address.

18 When operated as intended and required by Apple and under Apple's direction and control,
19 pursuant to Apple's software licenses, privacy policies, and other user agreements, Apple end user
20 devices, operated by end users, register their current locations with the APNs servers, operated by
21 Apple, with a request and reply message exchange. Apple's servers, including its APNs servers
22 operated by Apple, forward the encrypted message payloads to the receiving Apple devices.
23 Apple's APNs servers and Apple devices sending and receiving messages through iMessage and
24 FaceTime communicate using a TLS protocol.

25 Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message
26 Forwarding, and encryption for Apple Watch apps with streaming data use Apple's APNs/IDS to
27 support end-to-end encryption utilizing the same methods described above with respect to

iMessage and FaceTime. *See e.g.*, iMessage Security Overview, *Apple Platform Security*, May 2022, p. 157, available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; FaceTime security, *id.*, at 162; Handoff, *id.*, at 166; Universal Clipboard, *id.*, at 167; iPhone cellular call relay security, *id.*, at 168; iPhone Text Message Forwarding security, *id.*, at 168; System security for watchOS, *id.*, at 69. Thus, as with iMessage and FaceTime, Apple likewise directs or controls the performance of end users of its devices utilizing these other services and features. Apple has the right and ability to stop or limit use of these other services and features. Apple conditions use of Apple devices and software, including use of these other services and features and the benefits derived therefrom, upon agreeing to the above legal terms, including performance of the relevant acts of infringement carried out by its devices, for which Apple establishes the manner and timing of such performance.

2. '397 Patent - Direct infringement based on joint acts of multiple parties

In addition to infringing the '397 Patent directly based entirely on Apple's own acts, including Apple testing its products and otherwise executing the claimed methods in the course of product development and support, Apple has and continues to directly infringe the '397 Patent based on joint acts of multiple parties. Specifically, Apple has infringed and continues to infringe at least claim 1 of the '397 Patent under 35 U.S.C. § 271(a) by making, using, and operating within the United States the Accused '397 Instrumentalities that support and enable its iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data that also use the Apple Push Notification service ("APNs") and Apple Identity service ("IDS") to support end-to-end encryption, as well as by directing and controlling, and conditioning its customers' and end users' participation and use of and receipt of the benefits of iMessage, FaceTime, Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data, upon the performance of steps of claim 1 of the '397 Patent and establishing the manner or timing of that performance. See attached claim chart.

Apple maintains absolute control over the operation of its iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming data, including its operation of the software, servers, and databases that support such services. Users are required to sign up and agree to numerous terms and conditions unilaterally imposed by Apple, including in its user software licenses, account agreements (iTunes/Apple ID), and privacy agreements, in order to use them.

Apple begins its “iOS Software License Agreement” by stating that “BY USING YOUR IPHONE, IPAD or IPOD Touch (“iOS DEVICE”), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS.” See “Apple Inc. iOS Software License Agreement” (www.apple.com/legal/sla/docs/iOS112.pdf); see also Apple Inc. Software License Agreement for macOS High Sierra (www.apple.com/legal/sla/docs/macOS1013.pdf); iOS16 and iPadOS16 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS15 and iPadOS15 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS14 and iPadOS14 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS13 and iPadOS13 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS12 “Apple Inc. iOS Software License Agreement”; iOS10 “Apple Inc. iOS Software License Agreement”; iOS 9 “Apple Inc. iOS Software License Agreement”; iOS 8 “Apple Inc. iOS Software License Agreement;” “Apple Inc. Software License Agreement for macOS Ventura;” “Apple Inc. Software License Agreement for macOS Monterey;” “Apple Inc. Software License Agreement for macOS Big Sur;” “Apple Inc. Software License Agreement for macOS Catalina;” “Apple Inc. Software License Agreement for macOS Mojave;” “Apple Inc. Software License Agreement for macOS Sierra;” “Apple Inc. Software License Agreement for macOS El Capitan;” “Apple Inc. Software License Agreement for macOS Yosemite;” Apple watchOS Software License Agreement, all available at <https://www.apple.com/legal/sla/>.

The Apple iOS Software License Agreement, to which each Apple iOS device user wishing to have access to, receive the benefit of, and use iMessage and FaceTime must agree, also provides:

The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with

your iOS Device (“Original iOS Software”), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple (“iOS Software Updates”), whether in read only memory, on any other media or in any other form (the Original iOS Software and iOS Software Updates are collectively referred to as the “iOS Software”) are licensed, not sold, to you by Apple Inc. (“Apple”) for use only under the terms of this License. Apple and its licensors retain ownership of the iOS Software itself and reserve all rights not expressly granted to you. You agree that the terms of this License will apply to any Apple-branded app that may be built-in on your iOS Device, unless such app is accompanied by a separate license, in which case you agree that the terms of that license will govern your use of that app.

See “Apple Inc. iOS Software License Agreement” (www.apple.com/legal/sla/docs/iOS112.pdf); *see also* iOS16 and iPadOS16 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS15 and iPadOS15 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS14 and iPadOS14 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS13 and iPadOS13 “Apple Inc. iOS and iPadOS Software License Agreement”; iOS12 “Apple Inc. iOS Software License Agreement”; iOS11 “Apple Inc. iOS Software License Agreement”; iOS10 “Apple Inc. iOS Software License Agreement”; iOS 9 “Apple Inc. iOS Software License Agreement”; iOS 8 “Apple Inc. iOS Software License Agreement”; Apple watchOS Software License Agreement, all available at <https://www.apple.com/legal/sla/>.

Similarly, the Apple macOS software license agreement states:

The Apple software (including Boot ROM code), any third party software, documentation, interfaces, content, fonts and any data accompanying this License whether preinstalled on Apple-branded hardware, on disk, in read only memory, on any other media or in any other form (collectively the “Apple Software”) are licensed, not sold, to you by Apple Inc. (“Apple”) for use only under the terms of this License. Apple and/or Apple’s licensors retain ownership of the Apple Software itself and reserve all rights not expressly granted to you. You agree that the terms of this License will apply to any Apple-branded application software product that may be preinstalled on your Apple-branded hardware, unless such product is accompanied by a separate license, in which case you agree that the terms of that license will govern your use of that product.

See also Apple Inc. Software License Agreement for macOS High Sierra (www.apple.com/legal/sla/docs/macOS1013.pdf); “Apple Inc. Software License Agreement for macOS Ventura”; “Apple Inc. Software License Agreement for macOS Monterey;” “Apple Inc.

1 Software License Agreement for macOS Big Sur;” “Apple Inc. Software License Agreement for
 2 macOS Catalina;” “Apple Inc. Software License Agreement for macOS Mojave;” “Apple Inc.
 3 Software License Agreement for macOS Sierra;” “Apple Inc. Software License Agreement for
 4 macOS El Capitan;” “Apple Inc. Software License Agreement for macOS Yosemite;” all available
 5 at <https://www.apple.com/legal/sla/>.

6 Additionally, Apple requires each user of iMessage and FaceTime to register and obtain
 7 an Apple ID as a prerequisite to using these services. Prior to using the services, each user must
 8 first log in and then provide and allow Apple to access, store, and use the user’s unique identifier.
 9 These requirements are set forth in Apple’s software license agreements for both iOS and macOS:

10 Use of the App Store requires a unique user name and password combination,
 11 known as an Apple ID. An Apple ID is also required to access app updates and
 certain features of the iOS Software and Services.

* * *

12 Consent to Use of Data. When you use your device, your phone number and certain
 13 unique identifiers for your iOS Device are sent to Apple in order to allow others to
 14 reach you by your phone number when using various communication features of
 15 the iOS Software, such as iMessage and FaceTime. When you use iMessage, Apple
 may hold your messages in encrypted form for a limited period of time in order to
 ensure their delivery.

* * *

16 By using this software in connection with an Apple ID, or other Apple Service, you
 17 agree to the applicable terms of service for that Service, such as the latest Apple
 18 Media Services Terms and Conditions for the country in which you access such
 19 Services, which you may access and review at
<http://www.apple.com/legal/internet-services/itunes/ww/>.

20 “Apple Inc. iOS Software License Agreement” (www.apple.com/legal/sla/docs/iOS112.pdf); *see*
 21 *also* Apple Inc. Software License Agreement for macOS High Sierra
 22 (www.apple.com/legal/sla/docs/macOS1013.pdf); iOS16 and iPadOS16 “Apple Inc. iOS and
 23 iPadOS Software License Agreement”; iOS15 and iPadOS15 “Apple Inc. iOS and iPadOS
 24 Software License Agreement”; iOS14 and iPadOS14 “Apple Inc. iOS and iPadOS Software
 25 License Agreement”; iOS13 and iPadOS13 “Apple Inc. iOS and iPadOS Software License
 26 Agreement”; iOS12 “Apple Inc. iOS Software License Agreement”; iOS10 “Apple Inc. iOS
 27 Software License Agreement”; iOS 9 “Apple Inc. iOS Software License Agreement”; iOS 8

1 “Apple Inc. iOS Software License Agreement;” “Apple Inc. Software License Agreement for
 2 macOS Ventura;” “Apple Inc. Software License Agreement for macOS Monterey;” “Apple Inc.
 3 Software License Agreement for macOS Big Sur;” “Apple Inc. Software License Agreement for
 4 macOS Catalina;” “Apple Inc. Software License Agreement for macOS Mojave;” “Apple Inc.
 5 Software License Agreement for macOS Sierra;” “Apple Inc. Software License Agreement for
 6 macOS El Capitan;” “Apple Inc. Software License Agreement for macOS Yosemite;” all available
 7 at <https://www.apple.com/legal/sla/>.

8 Apple further requires end users to provide personal information and other identifying
 9 information to access services provided by Apple, including the iMessage and FaceTime services,
 10 and to receive benefits from such services:

11 Personal information is data that can be used to identify or contact a single person.
 12 You may be asked to provide your personal information anytime you are in contact
 13 with Apple or an Apple affiliated company. Apple and its affiliates may share this
 14 personal information with each other and use it consistent with this Privacy Policy.
 15 They may also combine it with other information to provide and improve our
 16 products, services, content, and advertising. You are not required to provide the
 17 personal information that we have requested, but, if you chose not to do so, in many
 18 cases we will not be able to provide you with our products or services or respond
 19 to any queries you may have.

20 * * *

21 We may collect information such as occupation, language, zip code, area code,
 22 unique device identifier, referrer URL, location, and the time zone where an Apple
 23 product is used so that we can better understand customer behavior and improve
 24 our products, services, and advertising.

25 <https://www.apple.com/privacy/privacy-policy/> (accessed in 2018); *see also* Messages & Privacy,
 26 available at <https://www.apple.com/legal/privacy/data/en/messages/>; FaceTime & Privacy,
 27 available at <https://www.apple.com/legal/privacy/data/en/face-time/>.

28 Based on at least the above facts, Apple directs or controls the performance of end users of
 its devices operating Apple’s iMessage and FaceTime services. Apple has the right and ability to
 stop or limit use of its iMessage and FaceTime services. Apple conditions use of Apple devices
 and software, including use of the iMessage and FaceTime services and the benefits derived
 therefrom, upon agreeing to the above legal terms, including performance of the relevant acts of

1 infringement carried out by its devices, for which Apple establishes the manner and timing of such
2 performance as set forth below.

3 The Apple iMessage and FaceTime services enable the end user Accused '397
4 Instrumentalities including iPhones, iPads, iPods, Apple Watches, Mac computers, when operated
5 by customers and end users, to send and receive secure messages over a telecommunications
6 network, i.e., the Internet, via the server Accused '397 Instrumentalities, including the APNs and
7 IDS servers operated by Apple. In its Answer, Apple has denied that it owns and operates the
8 APNs servers. (*See* Dkt. No. 38 at ¶56). MPH intends to seek discovery on the basis for Apple's
9 denial. To the extent Apple contracts with third parties who own or operate the servers which
10 perform the salient functionality, such operation is attributable to Apple.

11 More specifically, when operated as intended and required by Apple and under Apple's
12 direction and control, pursuant to Apple's software licenses, privacy policies, and other user
13 agreements, Apple end user devices, including iPhones, iPads, iPods, Apple Watches, and Mac
14 computers, establish a secure connection with one another by negotiating and exchanging keys
15 with one another according to a key exchange protocol through intermediate Apple servers
16 operated by Apple.

17 Intermediate Apple servers, including Apple's APNs servers operated by Apple, receive
18 encrypted message payloads sent by Apple devices to provide the iMessage and FaceTime
19 services. The encrypted message payloads are sent to the address of the intermediate Apple
20 servers, including the APNs servers.

21 A device token is a unique identifier assigned by Apple to a specific app on a specific
22 Apple device. Messages sent through iMessage and FaceTime include a device token that
23 identifies a unique app-device combination. Apple's servers, including its APNs servers operated
24 by Apple, are configured to decrypt and read these device tokens and use such tokens to locate the
25 intended recipients of a message.

26 Apple's servers, including its APNs servers operated by Apple, forward the encrypted
27 message payload to the receiving Apple device.

1 Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message
2 Forwarding, and encryption for Apple Watch apps with streaming data, use Apple's APNs/IDS to
3 support end-to-end encryption, utilizing the same methods described above with respect to
4 iMessage and FaceTime. *See e.g.*, iMessage Security Overview, *Apple Platform Security*, May
5 2022, p. 157, available at [https://help.apple.com/pdf/security/en_US/apple-platform-security-](https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf)
6 [guide.pdf](https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf); *See, e.g.*, FaceTime security, *id.*, at 162; *See*, Handoff, *id.*, at 166; *See*, Universal
7 Clipboard, *id.*, at 167; *See*, iPhone cellular call relay security, *id.*, at 168; *See*, iPhone Text Message
8 Forwarding security, *id.*, at 168; *See*, System security for watchOS, *id.*, at 69. Thus, as with
9 iMessage and FaceTime, Apple likewise directs or controls the performance of end users of its
10 devices utilizing these other services and features. Apple has the right and ability to stop or limit
11 use of these other services and features. Apple conditions use of Apple devices and software,
12 including use of these other services and features and the benefits derived therefrom, upon agreeing
13 to the above legal terms, including performance of the relevant acts of infringement carried out by
14 its devices, for which Apple establishes the manner and timing of such performance.

15 **3. '502 Patent - Indirect infringement under 35 U.S.C. § 271 (b)-(c)**

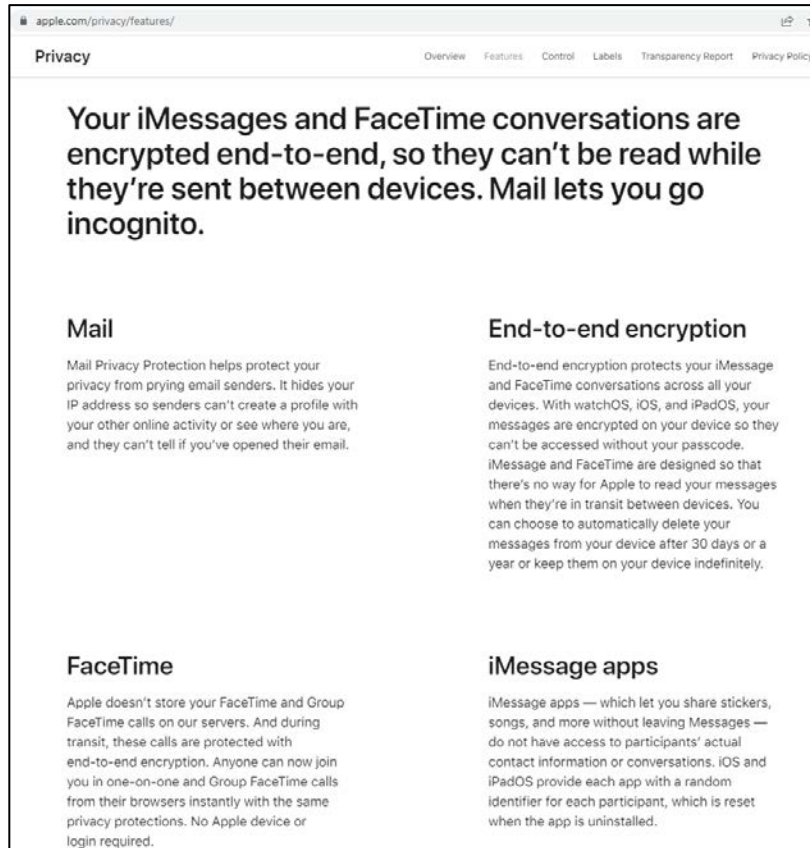
16 Apple has and continues to knowingly and actively induce infringement of at least claims
17 7, 8, and 9 of the '502 Patent under 35 U.S.C. §271(b) by, among other things, making, using,
18 selling, offering for sale, and importing within and into the United States the Accused '502
19 Instrumentalities, and by advertising, promoting, encouraging, instructing and aiding others, such
20 as resellers and end-user customers, to sell, offer to sell, and use the Accused '502 Instrumentalities
21 within the United States in an infringing matter via Apple's iMessage and FaceTime services, as
22 well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message
23 Forwarding, and encryption for Apple Watch apps with streaming data that also use Apple's
24 APNs/IDS to support end-to-end encryption, as shown in the attached claim chart. Such acts
25 constitute direct infringement.

26 Apple has had actual notice of its infringement of the '502 Patent by no later than July 18,
27 2017 when it received MPH's letter advising Apple of the '502 Patent and providing a claim chart

1 comparing the claims to Apple's iMessage and FaceTime services. (Dkt. No. 1, Compl. at ¶¶ 40-
2 41; Dkt. No. 38, Apple's Answer at ¶¶ 40-41). Apple has carried out these actions with the specific
3 intent to induce infringement of the '502 Patent and with knowledge that such acts constitute
4 infringement of the '502 Patent. Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone
5 Text Message Forwarding, and encryption for Apple Watch apps with streaming data also use
6 Apple's APNs/IDS to support end-to-end encryption and, thus, Apple further infringes the
7 foregoing claims of the '502 Patent under 35 U.S.C. § 271(b).

8 Resellers' and end-user customers' use, sales and offers to sell the Accused '502
9 Instrumentalities within the United States constitutes direct infringement of the apparatuses
10 claimed in claims 7, 8, and 9 of the '502 Patent. Apple has taken active steps to encourage direct
11 infringement of the '502 Patent by advertising the infringing uses and through Apple's instructions
12 of how to engage in infringing uses of the iMessage and FaceTime services, as well as Handoff,
13 Universal Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and
14 encryption for Apple Watch apps with streaming data that also use Apple's APNs/IDS to support
15 end-to-end encryption.

Apple touts its end-to-end encryption technology for iMessage and FaceTime:



Apple Privacy, <https://www.apple.com/privacy/features/>.

In its *Apple Platform Security* guide (May 2022) (with similar statements other versions of the *Apple Platform Security* guide, as well as Apple's *iOS Security* guides), Apple states that:

Apple iMessage is a messaging service for iOS and iPadOS devices, Apple Watch, and Mac computers. iMessage supports text and attachments such as photos, contacts, locations, links, and attachments directly on to a message, such as a thumbs up icon. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple doesn't log the contents of messages or attachments, which are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple can't decrypt the data.

See *Apple Platform Security*, May 2022, p. 157, available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf; *Apple Platform Security* (May 2021), p. 155; *Apple Platform Security* (Spring 2020), p. 99; *iOS Security*, iOS 12.3 (May 2019), p. 60, *iOS Security*, iOS12 (September 2018), p. 60; *iOS Security*, iOS 11 (January

2018), p. 54; *iOS Security*, iOS 10 (March 2017), p. 43; *iOS Security*, iOS 9.3 or later (May 2016), p. 41; *iOS Security*, iOS 9.0 or later (September 2015), p. 39; *iOS Security* (October 2014), p. 30-31; *see also* “Use Messages with your Mac,” available at <https://support.apple.com/en-us/HT202549> (“With messages for Mac, you can send unlimited messages to any Mac, iPhone, iPad, or iPod touch that uses iMessage, Apple’s secure-messaging service.”); macOS Security (March 2018), p. 1 (“For information on security features of Apple services not covered in this document, refer to the “iOS Security Guide” at www.apple.com/business/docs/iOS_Security_Guide.pdf.”); FaceTime security, *Apple Platform Security*, May 2022, p. 162 (“FaceTime is Apple’s video and audio calling service. Like iMessage, FaceTime calls use the Apple Push Notification service (APNs) to establish an initial connection to the user’s registered devices. The audio/video contents of FaceTime calls are protected by end-to-end encryption, so no one but the sender and receiver can access them. Apple can’t decrypt the data.”); Handoff, *id.*, at 166 (“With Handoff, when a user’s iOS, iPadOS, and macOS devices are near each other, the user can automatically pass whatever they’re working on from one device to the other. Handoff lets the user switch devices and instantly continue working. When a user signs in to iCloud on a second Handoff-capable device, the two devices establish a Bluetooth Low Energy (BLE) 4.2 pairing out-of-band using APNs. The individual messages are encrypted much like messages in iMessage are.”); Universal Clipboard, *id.*, at 167 (“Universal Clipboard leverages Handoff to securely transfer the content of a user’s clipboard across devices so they can copy on one device and paste on another. Content is protected in the same way as other Handoff data and is shared by default with Universal Clipboard unless the app developer chooses to disallow sharing.”); iPhone cellular call relay security, *id.*, at 168 (“When an incoming call arrives, all configured devices are notified using the Apple Push Notification service (APNs), with each notification using the same end-to-end encryption as iMessage.”); iPhone Text Message Forwarding security, *id.*, at 168 (“iPhone encrypts and forwards incoming SMS text messages to each device, utilizing the methods described in iMessage security overview.”); System security for watchOS, *id.*, at 69 (“To support apps that need streaming data, encryption is provided with methods described in FaceTime

1 security, using either the Apple Identity Service (IDS) provided by the paired iPhone or a direct
2 internet connection.”).

3 Apple has also contributed to the infringement of at least claims 7, 8, and 9 of the ’502
4 Patent under 35 U.S.C. § 271(c) by, among other things, making, using, selling, offering for sale,
5 and importing into the United States the Accused ’502 Instrumentalities, and by advertising,
6 promoting, encouraging, instructing and aiding others, such as end-user customers, to use them in
7 an infringing manner, as shown in the attached claim chart, via Apple’s iMessage and FaceTime
8 services, as well as Handoff, Universal Clipboard, iPhone Cellular Call Relay, iPhone Text
9 Message Forwarding, and encryption for Apple Watch apps with streaming data that also use
10 Apple’s APNs/IDS to support end-to-end encryption. *See, generally*, Apple’s advertisements,
11 guides, instructions, whitepapers, and training materials cited with respect to inducement, *supra*.
12 Such acts by end users constitute direct infringement. Apple has engaged in these activities
13 knowing that the Accused ’502 Instrumentalities are especially made and adapted for use, and in
14 fact used, in a manner that constitutes infringement of the ’502 Patent. (Dkt. No. 1, Compl. at ¶¶
15 40-41; Dkt. No. 38, Apple’s Answer at ¶¶40-41).

16 The Accused ’502 Instrumentalities constitute material parts of the patented inventions of
17 the ’502 Patent, which are not staple articles of commerce suitable for substantial non-infringing
18 uses. As of its Answer, Apple has admitted that it has implemented the accused iMessage platform
19 in at least the following operating systems that run on Apple devices: iOS 8, iOS 9, iOS 10, iOS
20 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave,
21 WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5. (Dkt. No. 1, Compl. at ¶51; Dkt. No. 38,
22 Apple’s Answer at ¶51). Apple has also admitted that FaceTime uses end-to-end encryption to
23 protect FaceTime audio and video contents, that Apple is unable to decrypt the data sent through
24 FaceTime, and that Apple has made FaceTime available on at least the following operating systems
25 that run on Apple devices: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan,
26 macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and
27 WatchOS 5. (Dkt. No. 1, Compl. at ¶¶53-54; Dkt. No. 38, Apple’s Answer at ¶¶53-54). Later

1 versions are also accused. *See* Accused '502 Instrumentalities and claim chart. Apple has further
2 admitted that other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call
3 Relay, and iPhone Text Message Forwarding, use APNs to support end-to-end encryption. (Dkt.
4 No. 1, Compl. at ¶59; Dkt. No. 38, Apple's Answer at ¶59).

5 In the Accused '502 Instrumentalities, the specific software operating in conjunction with
6 hardware to provide Apple's iMessage and FaceTime services, as well as Handoff, Universal
7 Clipboard, iPhone Cellular Call Relay, iPhone Text Message Forwarding, and encryption for
8 Apple Watch apps with streaming data that also use Apple's APNs/IDS to support end-to-end
9 encryption, has no substantial noninfringing uses other than to practice the '502 Patent claimed
10 apparatuses. The Apple iMessage, FaceTime, Handoff, Universal Clipboard, iPhone Cellular Call
11 Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with streaming
12 data capabilities of the Accused '502 Instrumentalities are separate and distinct from other
13 functions of the Accused '502 Instrumentalities. As shown in the attached claim chart for the '502
14 Patent, the Accused '502 Instrumentalities' specific software operating in conjunction with
15 hardware to provide Apple iMessage, FaceTime, Handoff, Universal Clipboard, iPhone Cellular
16 Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with
17 streaming data is a material part of the patented inventions.

18 The direct infringers for Apple's contributory infringement under 35 U.S.C. § 271(c)
19 include, without limitation, end users and resellers of the Accused '502 Instrumentalities.

20 **4. '362 and '494 Patents - Direct infringement based on joint acts of**
21 **multiple parties**

22 MPH presently contends that all steps of the claimed methods of the '362 and '494 patents
23 are performed by Apple via the Apple servers and associated software that support and enable
24 Apple's iMessage and FaceTime services, as well as Handoff, Universal Clipboard, iPhone
25 Cellular Call Relay, iPhone Text Message Forwarding, and encryption for Apple Watch apps with
26 streaming data. *See* Accused '362 Instrumentalities and Accused '494 Instrumentalities. Based on
27 presently available material, these servers include those supporting and enabling Apple's Push

1 Notification service. In its Answer, Apple has denied that it owns and operates the APNs servers.
2 (See Dkt. No. 38 at ¶56). MPH intends to seek discovery on the basis for Apple's denial. To the
3 extent Apple contracts with third parties who own or operate the servers which perform the salient
4 functionality, such operation is attributable to Apple.

5 **5. '581 Patent – Indirect infringement under 35 U.S.C. § 271 (b)-(c)**

6 Apple has and continues to knowingly and actively induce infringement of claims 6-8 of
7 the '581 Patent under 35 U.S.C. §271(b) by selling and offering for sale in the United States, and
8 importing into the United States, the Accused '581 Instrumentalities that provide IKEv2 type
9 VPNs and enable MOBIKE, and by advertising, aiding, encouraging and instructing business,
10 enterprise, school, organization, and other end-user customers, including those that use AppleCare
11 for Enterprise, Apple Business Manager, Apple School Manager, Apple Configurator, Apple
12 Configurator 2, and/or Device Enrollment Program, to use them in an infringing manner, as set
13 forth in the attached claim chart. Such direct infringers include customers such as corporations and
14 other entities setting up IKEv2 type MOBIKE enabled VPNs to allow users to securely access
15 resources remotely via the Accused '581 Instrumentalities.

16 Apple has had actual notice of its infringement of the '581 Patent since October 18, 2016
17 when it received MPH's letter advising Apple of the '581 Patent and a detailed claim chart. (Dkt.
18 No. 38, Apple's Answer at ¶¶ 27-29). In this October 18, 2016 communication, MPH informed
19 Apple of its ongoing infringement of the '581 Patent. MPH also provided a detailed claim chart
20 for the '581 Patent showing the relevance of the MPH patents to Apple's products, including
21 Apple's adoption of "MOBIKE" technologies in its iOS and OS X/macOS devices and services.
22 (Dkt. 1, Compl. at ¶¶ 27-29). Apple has carried out its infringing activities with the specific intent
23 to induce infringement of the '581 Patent and with knowledge that such acts constitute
24 infringement of the '581 Patent.

25 Apple has taken active steps to encourage direct infringement of the '581 Patent by
26 advertising the infringing uses and through Apple's instructions of how to engage in infringing
27 uses. In particular, Apple announced to the Internet Engineering Task Force back in 2015 that, for

VPN configurations in iOS and OS X, Apple was enabling MOBIKE (RFC 4555) by default and that IKEv2 was the default VPN type. See <https://www.ietf.org/mail-archive/web/ipsec/current/msg09931.html>. Apple has provided its *Apple Platform Deployment* guide, *iOS Deployment Reference*, and *macOS Deployment Reference* materials, as well as the *Apple Deployment and Management Tutorials (Using VPN on Apple Devices)*, to guide and instruct its customers and end users on how to deploy the Accused '581 Instrumentalities in private corporate networks using VPN protocols including IKEv2 and MOBIKE. See *Apple Platform Deployment, VPN overview for Apple device deployment*, available at <https://support.apple.com/guide/deployment/vpn-overview-depae3d361d0/1/web/1.0>; *iOS Deployment Reference, Virtual Private Networks (VPN) Supported protocols and authentication methods*, formerly available at <https://help.apple.com/deployment/ios/#/ior38e77f0cf>; *macOS Deployment Reference, Virtual Private Networks (VPN) Supported protocols and authentication methods*, formerly available at <https://help.apple.com/deployment/macOS/#/ior38e77f0cf>; *Deployment and Management Tutorials (Using VPN on Apple Devices)* available at <https://it-training.apple.com/tutorials/deployment/dm165>. Apple also provided its *iOS Deployment Reference* to guide and instruct its customers and end users on how to deploy the Accused '581 Instrumentalities including VPN Setup Guidelines with an IKEv2 setup. See *iOS Deployment Reference, VPN Setup Guidelines, IKEv2 setup*, formerly available at <https://help.apple.com/deployment/ios/#/ior0f9aea818>.

Apple further provides, and has provided, Apple Platform, iOS and macOS Security guides and whitepapers that encourage the use of Accused '581 Instrumentalities in virtual private networking, including with the IKEv2 protocol. See *Apple Platform Security*, May 2022, p. 173; See also, *iOS Security Guide*, Sept. 2015, p. 28; *iOS Security Guide*, May 2016, p. 29; *iOS Security Guide*, Mar. 2017, p. 31; *iOS Security Guide*, Jan. 2018, p. 37; *macOS Security Overview for IT*, Mar. 2018, p. 10; *iOS Security Guide*, Aug. 2018, p. 36; *iOS Security Guide*, Sept. 2018, p. 40; *iOS Security Guide*, Nov. 2018, p. 40; *iOS Security Guide*, May 2019, p. 40; *Apple Platform Security*, Spring 2020, p. 110-11; *Apple Platform Security*, Feb. 2021, p. 152; *Apple Platform*

1 *Security*, May 2021, p. 174. Further, Apple published the *iOS Deployment Overview for Business*,
 2 *iOS and iPadOS Deployment Overview*, and *Mac Deployment Overview* whitepapers to encourage
 3 customers and end users to use VPNs to securely access company resources remotely via their
 4 iOS, iPadOS, mac devices. *See iOS and iPadOS Deployment Overview*, December 2021, available
 5 at https://www.apple.com/business/docs/site/iOS_and_iPadOS_Deployment_Overview.pdf; *iOS*
 6 *Deployment Overview for Business*, October 2016, available at
 7 https://images.apple.com/ae/business/resources/docs/iOS_Deployment_Overview_Business.pdf;
 8 *Mac Deployment Overview*, December 2021, available at
 9 https://www.apple.com/business/docs/site/Mac_Deployment_Overview.pdf.

10 Apple also provides and has provided programs including Apple Configurator, Apple
 11 Configurator 2, Apple School Manager, Apple Business Manager, and Device Enrollment
 12 Program, and instructions for using the programs including, for example, to configure and
 13 supervise Accused '581 Instrumentalities for use in virtual private networking. *See Apple Platform*
 14 *Security*, May 2022, p. 173; *see also, iOS Security Guide*, Sept. 2015, p. 28; *iOS Security Guide*,
 15 May 2016, p. 29; *iOS Security Guide*, Mar. 2017, p. 31; *iOS Security Guide*, Jan. 2018, p. 37;
 16 *macOS Security Overview for IT*, Mar. 2018, pp. 10, 13; *iOS Security Guide*, Aug. 2018, p. 36;
 17 *iOS Security Guide*, Sept. 2018, p. 40; *iOS Security Guide*, Nov. 2018, p. 40; *iOS Security Guide*,
 18 May 2019, p. 40; *Apple Platform Security*, Spring 2020, p. 110-11; *Apple Platform Security*, Feb.
 19 2021, p. 152; *Apple Platform Security*, May 2021, p. 174.

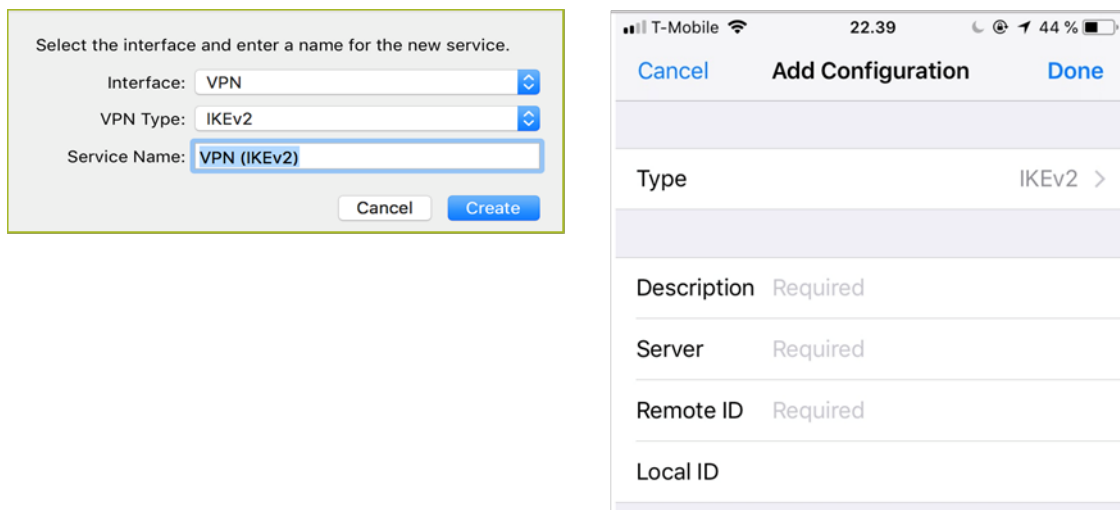
20 Apple also encourages infringing uses of the Accused '581 Instrumentalities on its website,
 21 where it advertises that Apple's Apple Business Manager solution can be used to easily configure
 22 Apple devices to allow employees to securely access a corporate network through built-in support
 23 for VPN, including IKEv2 networks:

24 VPN. Easily configure Apple devices for secure access to your corporate network
 25 through built-in support for VPN. Out of the box, iOS, iPadOS, and macOS support
 26 the industry-standard networks IKEv2, Cisco IPsec, and L2TP over Ipsec. Apple
 27 devices also support VPN On Demand, Always On VPN, and Per App VPN for
 facilitating connections on a much more granular basis for managed apps or specific
 domains. Whatever method your business chooses, data in transit is protected.

See Apple at Work, available at <https://www.apple.com/business/it/>.

With knowledge of the '581 Patent, Apple has also contributed to the infringement of claims 6-8 of the '581 Patent under 35 U.S.C. §271(c) by selling and offering for sale in the United States, and importing into the United States, the Accused '581 Instrumentalities, and by advertising, promoting, encouraging, instructing and aiding others, including its enterprise and other end-user customers, to use them in an infringing manner, namely, to provide IKEv2 type VPN and enable MOBIKE. *See, generally*, Apple's advertisements, guides, instructions, whitepapers, and training materials cited with respect to inducement, *supra*. Apple has engaged in these activities knowing that the Accused '581 Instrumentalities are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the '581 Patent. (Dkt. No. 38, Apple's Answer at ¶¶ 27-29).

The Accused '581 Instrumentalities constitute material parts of the patented inventions of the '581 Patent which are not staple articles of commerce suitable for substantial non-infringing uses. In the Accused '581 Instrumentalities, the specific software operating in conjunction with hardware to provide IKEv2 type VPN and enable MOBIKE has no substantial noninfringing uses other than to practice the '581 Patent claimed methods. Below are screenshots from macOS and iOS built-in VPN clients showing that IKEv2 type VPN is the default option:



The IKEv2 type MOBIKE enabled VPN capability of the Accused '581 Instrumentalities is

1 separate and distinct from other functions of the Accused '581 Instrumentalities. As shown in the
2 attached claim chart for the '581 Patent, the Accused '581 Instrumentalities' specific software
3 operating in conjunction with hardware to provide IKEv2 type VPN and enable MOBIKE is a
4 material part of the patented inventions.

5 The direct infringers for Apple's contributory infringement under 35 U.S.C. §271(c)
6 include users that use the Accused '581 Instrumentalities in an enterprise IKEv2 MOBIKE enabled
7 VPN to securely access resources remotely via the Accused '581 Instrumentalities including
8 business, enterprise, school, organization, and other end-user customers, including those that use
9 AppleCare for Enterprise, Apple's 24/7 support service that assists customers, Apple Business
10 Manager, Apple School Manager, Apple Configurator, Apple Configurator 2, and/or Device
11 Enrollment Program.

12 **6. '302 Patent - Indirect infringement under 35 U.S.C. § 271 (b)-(c)**

13 Apple has and continues to knowingly and actively induce infringement of claims 1, 2, 3,
14 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent under 35 U.S.C. § 271(b) by selling, offering for
15 sale, and importing in and into the United States the Accused '302 Instrumentalities that support
16 and enable Always-on VPN, as set forth in the attached claim chart, and by advertising, aiding,
17 encouraging and instructing others, such as its business, enterprise, school, organization and other
18 end-user customers, to use the Accused '302 Instrumentalities for Always-On VPN in a manner
19 that directly infringes claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent.

20 Apple has had actual notice of its infringement of the '302 Patent since October 18, 2016
21 when it received MPH's letter advising Apple of the '302 Patent. (Dkt. No. 38, Apple's Answer at
22 ¶¶ 27-29). On November 22, 2016, Apple received a claim chart from MPH comparing claims of
23 the '302 Patent to Apple's products with Always-On VPN. (*Id.* at ¶ 30). Apple has carried out its
24 infringing activities with the specific intent to induce infringement of the '302 Patent and with
25 knowledge that such acts constitute infringement of the '302 Patent.

26 Apple has taken active steps to encourage direct infringement of the '302 Patent by
27 advertising the infringing uses and through Apple's instructions of how to engage in infringing

1 uses of the Accused '302 Instrumentalities to support and enable Always-on VPN. In its Apple
 2 Platform Security guide dated May 2022 (with similar statements in earlier versions of the Apple
 3 Platform Security guide, as well as Apple's iOS Security guides), Apple states that:

4 iOS and iPadOS support the following:

5 *Always On VPN*: For devices managed through an MDM solution and supervised
 6 using Apple Configurator for Mac, Apple School Manager, or Apple Business
 7 Manager. Always On VPN eliminates the need for users to turn on VPN to enable
 8 protection when connecting to cellular and Wi-Fi networks. It also gives an
 9 organization full control over device traffic by tunneling all IP traffic back to the
 organization. The default exchange of parameters and keys for the subsequent
 encryption, IKEv2, secures traffic transmission with data encryption. The
 organization can monitor and filter traffic to and from its devices, secure data within
 its network, and restrict device access to the internet.

10 *Apple Platform Security*, May 2022, p. 173; *Apple Platform Security*, May 2021, p. 174; *Apple*
 11 *Platform Security*, Feb. 2021, p. 152; *Apple Platform Security*, Spring 2020, p. 110-11; *iOS*
 12 *Security Guide*, May 2019, p. 40; *iOS Security Guide*, Nov. 2018, p. 40; *iOS Security Guide*, Sept.
 13 2018, p. 40; *iOS Security Guide*, Aug. 2018, p. 36; *iOS Security Guide*, Jan. 2018, p. 37; *iOS*
 14 *Security Guide*, Mar. 2017, p. 31; *iOS Security Guide*, May 2016, p. 29; *iOS Security Guide*, Sept.
 15 2015, p. 28; *iOS Security*, Sept. 2014, p. 20-21 (iOS 8); *iOS Deployment Reference*, 2014, pp. 29,
 16 35-38.

17 Apple provides its *Apple Platform Deployment* guide and *iOS Deployment Reference*
 18 materials, as well as the *Apple Deployment and Management Tutorials (Using VPN on Apple*
 19 *Devices)*, to guide, instruct and encourage its customers and end users to deploy the Accused '302
 20 Instrumentalities in private corporate networks using Always-On VPN. See *Apple Platform*
 21 *Deployment, VPN overview for Apple device deployment*, available at
 22 <https://support.apple.com/guide/deployment/vpn-overview-depae3d361d0/1/web/1.0>; iOS
 23 Deployment Reference, Always-On VPN, formerly available at
 24 <https://help.apple.com/deployment/ios/#/ior9f7b5ff26>; *iOS Deployment Reference, Always-On*
 25 *VPN Configurations*, formerly available at
 26 <https://help.apple.com/deployment/ios/#/ior41cec49b6>; *iOS Deployment Reference*, 2014, pp. 29,
 27

35-38; *Deployment and Management Tutorials (Using VPN on Apple Devices)* available at <https://it-training.apple.com/tutorials/deployment/dm165>.

More specifically, Apple has provided its iOS Deployment Reference materials to guide and instruct its customers and end users on how to deploy the Accused '302 Instrumentalities in private corporate networks using Always-On VPN including providing guidance on Always-On VPN Configurations, the Always-On configuration profile, and the Always-On VPN payload. *See, e.g., iOS Deployment Reference*, 2014, pp. 29, 35-38. In the Apple iOS Deployment Reference, Apple states: "Once the Always-on VPN profile is installed on a device, Always-on VPN automatically activates with no user interaction. Always-on VPN stays activated (including across reboots) until the Always-on VPN profile is uninstalled." *Id.* Apple also states: "An Always-on VPN configuration profile can be composed either manually, using one of the Apple configuration profile editors such as Profile Manager or Apple Configurator, or a third party MDM vendor." *Id.*

Apple has further provided the *Managing Devices and Corporate Data on iOS* document, which states that "iOS features such as automated enrollment, lockable MDM settings, device supervision, and always-on VPN ensure that devices are configured based on your organization's specific requirements, providing increased control while ensuring that corporate data is protected." *See Managing Devices and Corporate Data on iOS*, p. 10 (July 2018), formerly available at https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf.

Apple also provides and has provided programs including Apple Profile Manager, Apple Configurator, Apple Configurator 2, Apple School Manager, Apple Business Manager, and Device Enrollment Program, and instructions for using the programs including, for example, to configure and supervise the Accused '302 Instrumentalities for using Always-On VPN. *Apple Platform Security*, May 2022, p. 173; *Apple Platform Security*, May 2021, p. 174; *Apple Platform Security*, Feb. 2021, p. 152; *Apple Platform Security*, Spring 2020, p. 110-11; *iOS Security Guide*, May 2019, p. 40; *iOS Security Guide*, Nov. 2018, p. 40; *iOS Security Guide*, Sept. 2018, p. 40; *iOS Security Guide*, Aug. 2018, p. 36; *iOS Security Guide*, Jan. 2018, p. 37; *iOS Security Guide*, Mar.

2017, p. 31; *iOS Security Guide*, May 2016, p. 29; *iOS Security Guide*, Sept. 2015, p. 28; *iOS Security*, Sept. 2014, p. 20-21 (iOS 8); *iOS Deployment Reference*, 2014, pp. 29, 35-38.

Apple also encourages infringing uses of the Accused '302 Instrumentalities on its website, where it advertises that Apple's Apple Business Manager solution can be used to easily configure Apple devices to allow employees to securely access a corporate network through built-in support for VPN, including Always On VPN:

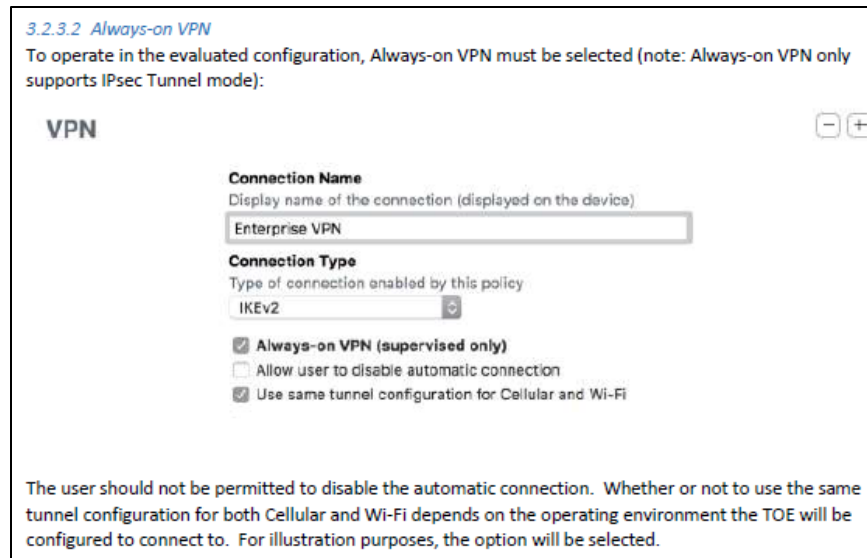
VPN. Easily configure Apple devices for secure access to your corporate network through built-in support for VPN. Out of the box, iOS, iPadOS, and macOS support the industry-standard networks IKEv2, Cisco IPsec, and L2TP over Ipsec. Apple devices also support VPN On Demand, Always On VPN, and Per App VPN for facilitating connections on a much more granular basis for managed apps or specific domains. Whatever method your business chooses, data in transit is protected.

See Apple at Work, available at <https://www.apple.com/business/it/>.

Apple's iOS and iPadOS software and corresponding mobile devices, including iPhones and iPads running iOS 9, 10, 11, and 12, and iOS/iPadOS 13, 14, and 15, were evaluated for Common Criteria Certifications from the National Information Assurance Partnership (NIAP). In conjunction with those evaluations, Apple provided iOS and iPadOS mobile devices and software, as well as documentation specifically instructing how to operate the evaluated iOS and iPadOS mobile devices with Always-On VPN and instructing users on VPN server/gateway settings, including to specify the IP address or hostname of the VPN server/gateway via "RemoteAddress." See Common Criteria Configuration Guides for Apple iOS 15: iPhones and Apple iPadOS 15: iPads (Version 1.2, 2021-05-25); Apple iOS 14: iPhones and Apple iPadOS 14: iPads (Version 1.0, 2021-05-25); Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices (Version 1.1, 2020-10-07); Apple iPad and iPhone Mobile Devices with iOS 12 (Version 1.7, 2019-03-12); Apple iOS 11 VPN Client on iPhone and iPad Guidance Documentation (April 2018, Version 1.2); Apple iOS 10.2 VPN Client on iPhone and iPad Guidance Documentation (July 2017, Version 1.0); Apple iOS VPN Client Guidance Documentation (March 2016, Version 1.0); *see also* <https://developer.apple.com/documentation/devicemanagement/vpn/ikev2?language=objc>.

Such documentation specifically instructs users how to configure Always-on VPN, *see*,

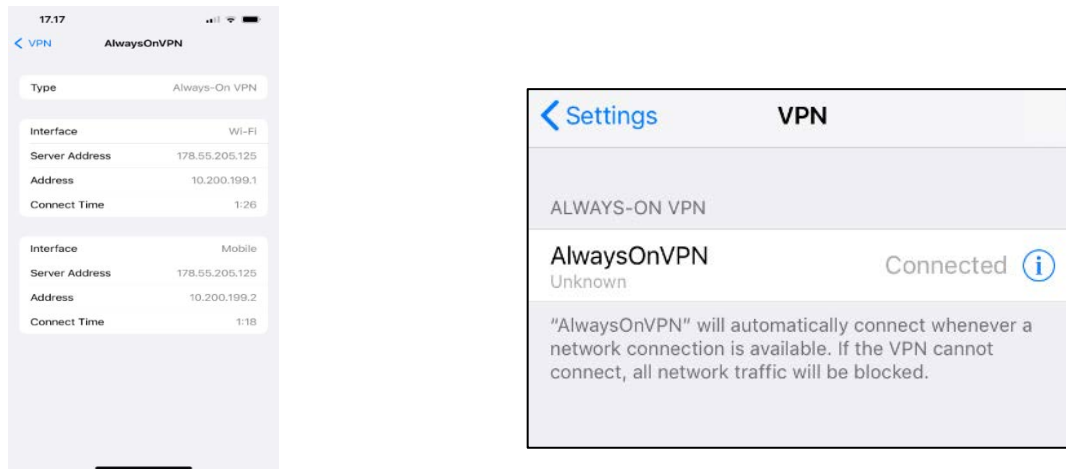
e.g., Apple iOS 11 VPN Client on iPhone and iPad Guidance Documentation (April 2018, Version 1.2), p. 12:



With knowledge of the '302 Patent, Apple has also contributed to the infringement of claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent under 35 U.S.C. § 271(c) by selling, offering for sale in the United States, and importing in and into the United States, the Accused '302 Instrumentalities, and by advertising, promoting, aiding, encouraging and instructing others, such as its business, enterprise and other end-user customers, to use the Accused '302 Instrumentalities for Always-On VPN in a manner that directly infringes claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent. *See, generally*, Apple's advertisements, guides, instructions, whitepapers, and training materials cited with respect to inducement, *supra*. Apple has engaged in these activities knowing that the Accused '302 Instrumentalities are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the '302 Patent. (Dkt. No. 38, Apple's Answer at ¶¶ 27-30).

The Accused '302 Instrumentalities constitute material parts of the patented inventions of the '302 Patent, which are not staple articles of commerce suitable for substantial non-infringing uses. As of its Answer, Apple has admitted that it introduced the Always-on VPN feature with its iOS 8 operating system, and that at least the iOS 8, iOS 9, iOS 10, iOS 11, and iOS 12 operating

systems support Always-on VPN capability. (See Dkt. No. 38 at ¶¶101-102). Later versions of iOS and iPad OS are also accused. See Accused '302 Instrumentalities and claim chart. In the Accused '302 Instrumentalities, the specific software operating in conjunction with hardware to provide Always-On VPN has no substantial noninfringing uses other than to practice the '302 Patent claimed methods. Below are exemplary screenshots from iOS 16 showing the Always-On VPN feature:



The Always-On VPN capability of the Accused '302 Instrumentalities is separate and distinct from other functions of the Accused '302 Instrumentalities. As shown in the attached claim chart for the '302 Patent, the Accused '302 Instrumentalities' specific software operating in conjunction with hardware to provide Always-On VPN is a material part of the patented inventions.

The direct infringers for Apple's contributory infringement of the '302 Patent under 35 U.S.C. § 271(c) include its business, enterprise, school, organization, and other end-user customers. See *Apple Platform Security*, May 2022, p. 173 (discussing use of MDM solutions, Apple School Manager, and Apple Business Manager to configure and supervise devices using Always-on VPN); *Managing Devices and Corporate Data on iOS*, p. 10 (July 2018), formerly available at https://www.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf.

E. Identification of Type of Infringement

MPH presently contends that each limitation of each asserted claim is literally present in the Accused Instrumentalities. MPH reserves the right to seek to amend these contentions pursuant to Local P.R. 3-6, including to assert infringement under the doctrine of equivalents based on any claim construction order issued by the Court.

F. Identification of Priority Dates

The asserted claims of the '581 Patent and '302 Patent are entitled to a priority date of September 28, 2001. The asserted claims of the '949 Patent, '397 Patent, '494 Patent, '502 Patent, and '362 Patent are entitled to a priority date of January 22, 2002.

G. MPH Products That Practice Claimed Inventions

MPH does not intend to rely on the assertion that its own or its licensees' apparatus, product, device, process, method, act, or other instrumentality practices the claimed inventions.

H. Infringement and Damages Period

MPH identifies the following dates of first infringement, start of claimed damages, and end of claimed damages for each asserted patent. MPH's identification of Apple's first date of infringement is based on public information available to MPH as of May 15, 2023 without the benefit of information to be produced by Apple pursuant to MPH's discovery requests served on May 1, 2023. MPH reserves the right to seek to amend its contentions with respect to the dates of first infringement by Apple based on information discovered in this case:

Asserted Patent	Point of First Infringement & Start of Claimed Damages	End of Claimed Damages
'949 Patent	First infringement and start of claimed damages: September 17, 2014	N/A (through present)
'397 Patent	Start of pre-issuance damages: October 18, 2016 First infringement of issued patent and start of post-issuance damages: September 12,	January 21, 2023

	2017	
'494 Patent	Start of pre-issuance damages: April 7, 2017 First infringement and start of post-issuance damages: July 18, 2017	January 21, 2023
'502 Patent	Start of pre-issuance damages: April 19, 2017 First infringement of issued patent and start of post-issuance damages: July 18, 2017	January 21, 2023
'362 Patent	Start of pre-issuance damages: September 21, 2017 First infringement of issued patent and start of post-issuance damages: December 5, 2017	January 21, 2023
'581 Patent	First infringement and start of claimed damages: October 18, 2016	September 27, 2022
'302 Patent	First infringement and start of claimed damages: September 17, 2014	N/A (through present)

I. Willful Infringement Allegations

The following contentions on willful infringement are based on the information known to MPH at this time (May 15, 2023) without the benefit of information to be produced by Apple pursuant to MPH's discovery requests served on May 1, 2023. MPH reserves all rights to supplement and/or amend its contentions pursuant to the Federal Rules of Civil Procedure, Orders of the Court, and Patent Local Rule 3-6.

1. '949 Patent

Apple's infringement of the '949 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights

1 including the '949 patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint.
2 For example, MPH notified Apple that it had and continued to infringe the '949 Patent in a detailed
3 letter dated October 18, 2016. On November 22, 2016, MPH also provided detailed claim charts
4 for the '949 Patent showing how Apple's iMessage service infringed the '949 Patent.

5 On September 27, 2018, after Apple had refused to enter into a license agreement with
6 MPH that would allow Apple to practice the inventions of the '949 patent with MPH's consent
7 and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '949 patent
8 after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged
9 invalidity of the '949 patent on the basis that U.S. Patent No. 7,181,612 to Pellacuru et al. and U.S.
10 Patent No. 7,159,109 to Egevang anticipated or rendered obvious the asserted claims of the '949
11 patent under 35 U.S.C. §§ 102 and 103. In March 2019, Apple filed an *inter partes* review petition
12 with the Patent Trial and Appeal Board ("PTAB") of the U.S. Patent Office arguing that each of
13 the asserted claims of the '949 patent was invalid. Based on this and other IPR petitions filed in
14 March 2019, Apple successfully sought a stay of this lawsuit, which was then stayed from April
15 2019 to February 2023. Although Apple's November 26, 2018 Answer and Counterclaims alleged
16 invalidity of the '949 patent based on Pellacuru and Egevang, Apple's March 2019 IPR petition
17 abandoned its invalidity theory set forth in the Answer and Counterclaims, and relied on other
18 alleged prior art. The U.S. Patent Office denied institution for the requested IPR of the '949 patent
19 in October 2019. Despite its knowledge of its infringement and the abandonment and rejection of
20 its invalidity allegations, Apple's infringement of the '949 patent continues without abatement.

21 **2. '397 Patent**

22 Apple's infringement of the '397 Patent has been and continues to be willful, wanton,
23 malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged
24 Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights
25 including the '397 patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint.
26 For example, MPH notified Apple of the application that later issued as the '397 Patent (U.S.
27 Patent Application No. 13/685,544) on October 18, 2016. On March 6, 2017, MPH also sent Apple

1 a detailed claim chart mapping allowed claim 1 of Application No. 13/685,544 to Apple's
2 iMessage. Then, on April 7, 2017, MPH gave Apple a copy of the published application
3 (Publication No. US 2017/0093580A9) that issued as the '397 Patent and the corresponding Notice
4 of Allowance issued by the U.S. Patent and Trademark Office.

5 On September 27, 2018, after Apple had refused to enter into a license agreement with
6 MPH that would allow Apple to practice the inventions of the '397 patent with MPH's consent
7 and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '397 patent
8 after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged
9 invalidity of the '397 patent on the basis that U.S. Patent No. 7,181,612 to Pellacuru et al. and U.S.
10 Patent No. 7,159,109 to Egevang anticipated or rendered obvious the asserted claims of the '397
11 patent under 35 U.S.C. §§ 102 and 103. In March 2019, Apple filed an *inter partes* review petition
12 with the Patent Trial and Appeal Board ("PTAB") of the U.S. Patent Office arguing that each of
13 the asserted claims of the '397 patent was invalid. Based on this and other IPR petitions filed in
14 March 2019, Apple successfully sought a stay of this lawsuit, which was then stayed from April
15 2019 to February 2023. Although Apple's November 26, 2018 Answer and Counterclaims alleged
16 invalidity of the '397 patent based on Pellacuru and Egevang, Apple's March 2019 IPR petition
17 abandoned its invalidity theory set forth in the Answer and Counterclaims, and relied on other
18 alleged prior art. The U.S. Patent Office denied institution for the requested IPR of the '397 patent
19 in November 2019. Despite its knowledge of its infringement and the abandonment and rejection
20 of its invalidity allegations, Apple's infringement of the '397 patent continued without abatement.

21 3. '494 Patent

22 Apple's infringement of the '494 Patent has been and continues to be willful, wanton,
23 malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged
24 Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights
25 including the '494 Patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint.
26 For example, MPH notified Apple that the application that later issued as the '494 Patent (U.S.
27 Patent Application No. 15/372,208; Publication No. US 2017/0093799 A1) had been allowed by

1 the Patent Office on April 7, 2017. MPH then notified Apple that it infringed the '494 Patent on
2 July 18, 2017 and provided claim charts comparing the claims to Apple's iMessage and FaceTime
3 services.

4 On September 27, 2018, after Apple had refused to enter into a license agreement with
5 MPH that would allow Apple to practice the inventions of the '494 Patent with MPH's consent
6 and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '494 Patent
7 after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged
8 invalidity of the '494 Patent on the basis that U.S. Patent No. 7,181,612 to Pellacuru et al. and U.S.
9 Patent No. 7,159,109 to Egevang anticipated or rendered obvious the asserted claims of the '494
10 Patent under 35 U.S.C. §§ 102 and 103. In March 2019, Apple filed an *inter partes* review petition
11 with the Patent Trial and Appeal Board ("PTAB") of the U.S. Patent Office arguing that each of
12 the asserted claims of the '494 Patent was invalid. Based on this and other IPR petitions filed in
13 March 2019, Apple successfully sought a stay of this lawsuit, which was then stayed from April
14 2019 to February 2023. Although Apple's November 26, 2018 Answer and Counterclaims alleged
15 invalidity of the '494 Patent based on Pellacuru and Egevang, Apple's March 2019 IPR petition
16 abandoned its invalidity theory set forth in the Answer and Counterclaims, and relied on other
17 alleged prior art. In the Final Written Decision entered on November 4, 2020, the PTAB
18 determined that Apple has not shown by a preponderance of the evidence that claims 2, 4, 9, and
19 11 of the '494 Patent are unpatentable. On March 9, 2022, the Federal Circuit affirmed the PTAB's
20 Final Written Decision. Despite its knowledge of its infringement and the abandonment and
21 rejection of its invalidity allegations by the PTAB and the Federal Circuit, Apple's infringement
22 of the '494 Patent continued without abatement.

23 4. '502 Patent

24 Apple's infringement of the '502 Patent has been and continues to be willful, wanton,
25 malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged
26 Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights
27 including the '502 patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint.

1 For example, MPH notified Apple of the published patent application that issued as the '502 Patent
2 (Publication No. US 2017/0099266A1) on April 19, 2017 and its relevance to various aspects of
3 Apple's iMessage and FaceTime services. MPH also contacted Apple on July 18, 2017 after the
4 '502 Patent issued, informing it once again of its infringement and providing claim charts
5 comparing the '502 Patent claims to Apple's iMessage and FaceTime services.

6 On September 27, 2018, after Apple had refused to enter into a license agreement with
7 MPH that would allow Apple to practice the inventions of the '502 patent with MPH's consent
8 and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '502 patent
9 after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged
10 invalidity of the '502 patent on the basis that U.S. Patent No. 7,181,612 to Pellacuru et al. and U.S.
11 Patent No. 7,159,109 to Egevang anticipated or rendered obvious the asserted claims of the '502
12 patent under 35 U.S.C. §§ 102 and 103. In March 2019, Apple filed an *inter partes* review petition
13 with the Patent Trial and Appeal Board ("PTAB") of the U.S. Patent Office arguing that each of
14 the asserted claims of the '502 patent was invalid. Based on this and other IPR petitions filed in
15 March 2019, Apple successfully sought a stay of this lawsuit, which was then stayed from April
16 2019 to February 2023. Although Apple's November 26, 2018 Answer and Counterclaims alleged
17 invalidity of the '502 patent based on Pellacuru and Egevang, Apple's March 2019 IPR petition
18 abandoned its invalidity theory set forth in the Answer and Counterclaims, and relied on other
19 alleged prior art. In the Final Written Decision entered on November 4, 2020, the PTAB
20 determined that Apple has not shown by a preponderance of the evidence that claims 7-9 of the
21 '502 patent are unpatentable. On March 9, 2022, the Federal Circuit affirmed the PTAB's Final
22 Written Decision. Despite its knowledge of its infringement and the abandonment and rejection of
23 its invalidity allegations by the PTAB and the Federal Circuit, Apple's infringement of the '502
24 patent continued without abatement.

25 **5. '362 Patent**

26 Apple's infringement of the '362 Patent has been and continues to be willful, wanton,
27 malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged

1 Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights
2 including the '362 patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint.
3 For example, MPH notified Apple of the pendency of U.S. Patent Application No. 15/609,312,
4 which issued as the '362 Patent, on July 18, 2017. Despite knowledge of its infringement of the
5 related '949, '397, '494 and '502 Patents, as well as the application which issued as the '362 Patent,
6 Apple continued its acts of infringement of the '362 Patent.

7 On September 27, 2018, after Apple had refused to enter into a license agreement with
8 MPH that would allow Apple to practice the inventions of the '362 patent with MPH's consent
9 and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '362 patent
10 after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged
11 invalidity of the '362 patent on the basis that U.S. Patent No. 7,181,612 to Pellacuru et al. and U.S.
12 Patent No. 7,159,109 to Egevang anticipated or rendered obvious the asserted claims of the '362
13 patent under 35 U.S.C. §§ 102 and 103. In March 2019, Apple filed an *inter partes* review petition
14 with the Patent Trial and Appeal Board ("PTAB") of the U.S. Patent Office arguing that each of
15 the asserted claims of the '362 patent was invalid. Based on this and other IPR petitions filed in
16 March 2019, Apple successfully sought a stay of this lawsuit, which was then stayed from April
17 2019 to February 2023. Although Apple's November 26, 2018 Answer and Counterclaims alleged
18 invalidity of the '362 patent based on Pellacuru and Egevang, Apple's March 2019 IPR petition
19 abandoned its invalidity theory set forth in the Answer and Counterclaims, and relied on other
20 alleged prior art. In the Final Written Decision entered on November 4, 2020, the PTAB
21 determined that Apple has not shown by a preponderance of the evidence that claims 3, 5, 10 and
22 12-16 of the '362 patent are unpatentable. On March 9, 2022, the Federal Circuit affirmed the
23 PTAB's Final Written Decision. Despite its knowledge of its infringement and the abandonment
24 and rejection of its invalidity allegations by the PTAB and the Federal Circuit, Apple's
25 infringement of the '362 patent continued without abatement.

1 **6. '581 Patent**

2 Apple's infringement of the '581 Patent has been and continues to be willful, wanton,
3 malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged
4 Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights
5 including the '581 Patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint.
6 For example, MPH notified Apple that it infringed the '581 Patent through an October 18, 2016
7 letter and provided detailed claim charts showing the relevance of the '581 Patent to Apple's
8 adoption of "MOBIKE" technologies (IETF RFC4555) in its iOS and OS X/macOS devices. With
9 full awareness of the '581 Patent, and despite the knowledge that its actions would induce others
10 to infringe and contribute to the infringement of others of the '581 Patent, Apple continued selling,
11 offering for sale and importing into the United States the Accused '581 Instrumentalities.

12 On September 27, 2018, after Apple had refused to enter into a license agreement with
13 MPH that would allow Apple to practice the inventions of the '581 Patent with MPH's consent
14 and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '581 Patent
15 after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged
16 invalidity of the '581 Patent on the basis that an alleged document named "Application-Centric
17 Analysis of IP-based Mobility Management Techniques" by Archan Misra, Subir Das, and
18 Prathima Agrawal ("Misra") and U.S. Patent No. 6,091,951 to Sturniolo et al. ("Sturniolo")
19 anticipated or rendered obvious the asserted claims of the '581 Patent under 35 U.S.C. §§ 102 and
20 103. In March 2019, Apple filed an *inter partes* review petition with the Patent Trial and Appeal
21 Board ("PTAB") of the U.S. Patent Office arguing that each of the asserted claims of the '581
22 patent was invalid. Based on this and other IPR petitions filed in March 2019, Apple successfully
23 sought a stay of this lawsuit, which was then stayed from April 2019 to February 2023. Although
24 Apple's November 26, 2018 Answer and Counterclaims alleged invalidity of the '581 patent based
25 on Misra and Sturniolo, Apple's March 2019 IPR petition abandoned its invalidity theory set forth
26 in the Answer and Counterclaims, and relied on other alleged prior art. In the Final Written
27 Decision entered on September 24, 2020, the PTAB determined that Apple had not shown by a

preponderance of the evidence that claims 4 and 6-8 of the '581 Patent are unpatentable. On September 8, 2022, the Federal Circuit affirmed that portion of the PTAB's Final Written Decision. Despite its knowledge of its infringement and the abandonment and rejection of its invalidity allegations by the PTAB and the Federal Circuit, Apple's infringement of the '581 Patent continued without abatement.

7. '302 Patent

Apple's infringement of the '302 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH in good faith engaged Apple in extensive pre-lawsuit discussions in the hopes of amicably licensing its patent rights including the '302 patent as set forth in Paragraphs 26 – 46 of its September 27, 2018 Complaint. For example, MPH notified Apple that it infringed the '302 Patent through an October 18, 2016 letter. On November 22, 2016, MPH's counsel provided detailed claim charts showing how Apple infringed the '302 Patent through its Always-On VPN feature. Despite knowledge of its infringement, Apple continues to infringe the '302 patent.

On September 27, 2018, after Apple had refused to enter into a license agreement with MPH that would allow Apple to practice the inventions of the '302 patent with MPH's consent and approval, MPH brought this lawsuit against Apple. Apple continued to infringe the '302 patent after the filing of the lawsuit. In its November 26, 2018 Answer and Counterclaims, Apple alleged invalidity of the '302 Patent on the basis that U.S. Patent No. 6,976,177 to Ahonen, U.S. Patent No. 6,904,466 to Ishiyama et al. and International Publication No. WO2000041427 to Rinman et al. anticipated or rendered obvious the asserted claims of the '302 Patent under 35 U.S.C. §§ 102 and 103. In March 2019, Apple filed an *inter partes* review petition with the Patent Trial and Appeal Board ("PTAB") of the U.S. Patent Office arguing that each of the asserted claims of the '302 patent was invalid. Based on this and other IPR petitions filed in March 2019, Apple successfully sought a stay of this lawsuit, which was then stayed from April 2019 to February 2023. Although Apple's November 26, 2018 Answer and Counterclaims alleged invalidity of the '302 patent based on Ahonen, Ishiyama and Rinman, Apple's March 2019 IPR petition pursued

different invalidity theories, and relied instead on Ahonen, Ishiyama and Gupta references. In the Final Written Decision entered on October 5, 2020, the PTAB determined that Apple had not shown by a preponderance of the evidence that claims 1-16 of the '302 patent are unpatentable. On January 25, 2022, the Federal Circuit affirmed the PTAB's Final Written Decision. Despite its knowledge of its infringement and the rejection of its invalidity allegations by the PTAB and the Federal Circuit, Apple's infringement of the '302 patent continues without abatement.

II. Patent Local Rule 3-2 Document Production

The following documents have been produced concurrently with these disclosures. MPH reserves the right to supplement this production as discovery progresses and as allowed by the Local Rules and upon Order of the Court.

(a) Documents (e.g., contracts, purchase orders, invoices, advertisements, marketing materials, offer letters, beta site testing agreements, and third party or joint development agreements) sufficient to evidence each discussion with, disclosure to, or other manner of providing to a third party, or sale of or offer to sell, or any public use of, the claimed invention prior to the date of application for the patent in suit. A party's production of a document as required herein shall not constitute an admission that such document evidences or is prior art under 35 U.S.C. § 102;

MPH is not aware of any responsive documents.

(b) All documents evidencing the conception, reduction to practice, design, and development of each claimed invention, which were created on or before the date of application for the patent in suit or the priority date identified pursuant to Patent L.R. 3-1(f), whichever is earlier;

MPH is not aware of any nonprivileged responsive documents.

(c) A copy of the file history for each patent in suit;

Produced as MPH00000062–520, MPH00000569–965, MPH00001095–1621, MPH00001708–2259, MPH00002415–2843, MPH00003054–3424, and MPH00003966–4690.

1 (d) All documents evidencing ownership of the patent rights by the party asserting patent
2 infringement;

3 **Produced as MPH00000521–532, MPH00001036–1039, MPH00001670–1674,**
4 **MPH00002331–2335, MPH00002910–2914, MPH00003425–3431, MPH00003954–3965, and**
5 **MPH00004769–4774.**

6 (e) If a party identifies instrumentalities pursuant to Patent L.R. 3-1(g), documents
7 sufficient to show the operation of any aspects or elements of such instrumentalities the patent
8 claimant relies upon as embodying any asserted claims;

9 **Not applicable.**

10 (f) All agreements, including licenses, transferring an interest in any patent-in-suit;

11 **Produced as MPH00004860–4904. See also documents identified above at Patent L.R.**
12 **3-2(d).**

13 (g) All agreements that the party asserting infringement contends are comparable to a
14 license that would result from a hypothetical reasonable royalty negotiation;

15 **MPH does not have any agreements in its possession, custody, or control that it**
16 **presently contends are comparable to a license that would result from a hypothetical**
17 **reasonable royalty negotiation. MPH intends to seek such documents from Apple and third**
18 **parties during the course of discovery.**

19 (h) All agreements that otherwise may be used to support the party asserting
20 infringement's damages case;

21 **MPH does not presently have any such agreements in its possession, custody, or**
22 **control that it may use to support its damages case. MPH intends to seek, and has sought,**
23 **such documents from Apple and third parties during the course of discovery.**

24 (i) If a party identifies instrumentalities pursuant to Patent L.R. 3-1(g), documents
25 sufficient to show marking of such embodying accused instrumentalities and if it wants to
26 preserve the right to recover lost profits based on such products, sales, revenues, costs and profits
27 of such embodying accused instrumentalities; and

1 **Not applicable.**

2 (j) All documents comprising or reflecting a F/RAND commitment or agreement with
3 respect to the asserted patent(s).

4 **Not applicable.**

5
6
7 Respectfully submitted,
 /s/

/Brian E. Haan/

8 Patricia L. Peden, Esq. (SBN 206440)
9 ppeden@bwslaw.com
10 BURKE, WILLIAMS & SORENSEN, LLP
11 1999 Harrison Street, Suite 1650
 Oakland, CA 94612
 Phone: (510) 273.8780
 Fax: (510) 839.9104

12 Christopher J. Lee (*pro hac vice*)
13 clee@leesheikh.com
14 David J. Sheikh (*pro hac vice*)
15 dsheikh@leesheikh.com
16 Brian E. Haan (*pro hac vice*)
17 bhaan@leesheikh.com
18 Ashley E. LaValley (*pro hac vice*)
19 alavalley@leesheikh.com
20 Dragan Gjorgiev (*pro hac vice*)
 dgjorgiev@leesheikh.com
 James D. Mitchell (*pro hac vice*)
 jmittchell@leesheikh.com
 LEE SHEIKH & HAAN LLC
 125 South Clark Street, Suite 1175
 Chicago, IL 60603
 Phone: (312) 982-0070
 Fax: (312) 982-0071

21 Attorneys for Plaintiff
22 MPH TECHNOLOGIES OY
23
24
25
26
27

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on May 15, 2023 the foregoing:

PLAINTIFF'S PATENT L.R. 3.1 DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS

was served via electronic transmission on all counsel of record.

I certify that all parties in this case are represented by counsel who are CM/ECF participants.

/Brian E. Haan/

Attorneys for Plaintiff
MPH TECHNOLOGIES OY